Part No. 060635-10, Rev. A
January 2020

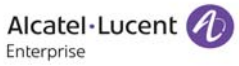
OmniSwitch AOS Release 8 CLI Reference Guide

8.6R2

Alcatel·Lucent Enterprise

www.al-enterprise.com

This user guide documents AOS Release 8.6R2.
The functionality described in this guide is subject to change without notice.



26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505

Service & Support Contact Information
North America: 800-995-2696
Latin America : 877-919-9526
EMEA : +800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific: +65 6240 8484
Web: businessportal2.alcatel-lucent.com
Email: ebg_global_supportcenter@al-enterprise.com

Contents

About This Guide

This *OmniSwitch AOS Release 8 CLI Reference Guide* is a comprehensive resource to all Command Line Interface (CLI) commands available on the OmniSwitch.

Supported Platforms

The information in this guide applies only to the following products:

- OmniSwitch 6465 Series
- OmniSwitch 6560 Series
- OmniSwitch 6860 Series
- OmniSwitch 6865 Series
- OmniSwitch 6900 Series
- OmniSwitch 9900 Series

Who Should Read this Manual?

The audience for this user guide is network administrators and IT support personnel who need to configure, maintain, and monitor switches and routers in a live network. Anyone wishing to gain knowledge on the details of all CLI commands available on the OmniSwitch will benefit from the material in this reference guide. However, advanced users who have already familiarized themselves with the OmniSwitch CLI commands will benefit most from the detailed content in this guide.

When Should I Read this Manual?

Read this guide whenever you want detailed information on individual CLI commands. Although this guide provides helpful information during any stage of the configuration process, it is a good idea to first familiarize yourself with the software features available on the switch before investigating the detailed command information in this guide.

Overview information, procedures, and live network examples on switch software features can be found in the *OmniSwitch AOS Release 8 Switch Management Guide, OmniSwitch AOS Release 8 Network Configuration Guide, OmniSwitch AOS Release 8 Advanced Routing Configuration Guide,* and *OmniSwitch AOS Release 8 Data Center Switching Guide.* Once you are familiar with the procedures and base CLI commands in these configuration guides you can obtain more detailed information on the individual commands in this guide.

What is in this Manual?

This reference guide includes information on every CLI command available in the switch. Command reference information is included for base software commands as well as commands associated with optional software packages, such as Advanced Routing (multicast routing protocols and OSPF). The information provided for each CLI command includes:

- Command description.
- Syntax.
- Description of all keywords and variables included in the syntax.
- Default values.
- Usage guidelines, which include tips on when and how to use the command.
- Examples of command lines using the command.
- Related commands with descriptions.
- Release history, which indicates the release when the command was introduced.
- SNMP information, such as the MIB files related to a set of CLI commands. In addition each CLI command includes the corresponding MIB variables that map to all parameters included in a command.

What is Not in this Manual?

Primarily a reference, this guide does not provide step-by-step instructions on how to set up particular features on the switch. It also does not provide overview or application examples on software features. For comprehensive information on how to configure particular software features in the switch, consult the appropriate configuration guide.

This guide also does not provide any information on the network management applications, WebView and OmniVista. Further information on WebView and OmniVista can be found in the context-sensitive on-line help available with those applications.

How is the Information Organized?

Each chapter in this guide includes reference material for all commands related to a single software feature, such as server load balancing or link aggregation. Typically commands in a single chapter will share a common prefix.

Text Conventions

The following table contains text conventions and usage guidelines for CLI commands as they are documented in this guide.

bold text	Indicates basic command and keyword syntax. Example: **show snmp station**
italicized text	Indicates user-specific information such as IP addresses, slot numbers, passwords, names, etc. Example: **no snmp station** *ip_address* Italicized text that is not enclosed with straight brackets (**[ ]**) indicates required information.
[ ] (Straight Brackets)	Indicates optional parameters for a given command. Example: **show aaa server [***server_name***]** Here, you can enter either of the following options: **show aaa server** **show aaa server** *server_name* (where *server_name* is the user-specified server name, e.g., **show aaa server myserver1**) Note that this example includes *italicized text*. The optional parameter in this case is a user-specified server name.
{ } (Curly Braces)	Indicates that the user must choose between one or more parameters. Example: **port mirroring {enable | disable}** Here, you must choose one of the following: **port mirroring enable** or **port mirroring disable**
| (Vertical Pipes)	Used to separate parameter choices within a command string. For example, the command string **show health threshold [rx | txrx | memory | cpu]** separates the choices **rx**, **txrx**, **memory,** and **cpu**. Examples: **show health threshold rx** **show health threshold txrx** **show health threshold memory** **show health threshold cpu**
“ ” (Quotation Marks)	Used to enclose text strings that contain spaces. The quotation marks are required input on the command line. Example: **vlan 2 “new test vlan”**

Documentation Roadmap

The OmniSwitch user documentation suite was designed to supply you with information at several critical junctures of the configuration process.The following section outlines a roadmap of the manuals that will help you at each stage of the configuration process. Under each stage, we point you to the manual or manuals that will be most helpful to you.

Stage 1: Using the Switch for the First Time

Pertinent Documentation: *OmniSwitch Hardware Users Guide*
Release Notes

This guide provides all the information you need to get your switch up and running the first time. It provides information on unpacking the switch, rack mounting the switch, installing NI modules, unlocking access control, setting the switch's IP address, and setting up a password. It also includes succinct overview information on fundamental aspects of the switch, such as hardware LEDs, the software directory structure, CLI conventions, and web-based management.

At this time you should also familiarize yourself with the Release Notes that accompanied your switch. This document includes important information on feature limitations that are not included in other user guides.

Stage 2: Gaining Familiarity with Basic Switch Functions

Pertinent Documentation: *OmniSwitch Hardware Users Guide*
OmniSwitch AOS Release 8 Switch Management Guide

Once you have your switch up and running, you will want to begin investigating basic aspects of its hardware and software. Information about switch hardware is provided in the *OmniSwitch Hardware Users Guide*. This guide provide specifications, illustrations, and descriptions of all hardware components, such as chassis, power supplies, Chassis Management Modules (CMMs), Network Interface (NI) modules, and cooling fans. It also includes steps for common procedures, such as removing and installing switch components.

The *OmniSwitch AOS Release 8 Switch Management Guide* is the primary users guide for the basic software features on a single switch. This guide contains information on the switch directory structure, basic file and directory utilities, switch access security, SNMP, and web-based management. It is recommended that you read this guide before connecting your switch to the network.

Stage 3: Integrating the Switch Into a Network

Pertinent Documentation: *OmniSwitch AOS Release 8 Network Configuration Guide*
OmniSwitch AOS Release 8 Advanced Routing Configuration Guide
OmniSwitch AOS Release 8 Data Center Switching Guide

When you are ready to connect your switch to the network, you will need to learn how the OmniSwitch implements fundamental software features, such as 802.1Q, VLANs, Spanning Tree, and network routing protocols. The *OmniSwitch AOS Release 8 Network Configuration Guide* contains overview information, procedures, and examples on how standard networking technologies are configured on the OmniSwitch.

The *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide* includes configuration information for networks using advanced routing technologies (OSPF and BGP) and multicast routing protocols (DVMRP and PIM-SM).

The *OmniSwitch AOS Release 8 Data Center Switching Guide* includes configuration information for data center networks using virtualization technologies, such as Data Center Bridging (DCB) protocols, Virtual eXtensible LAN (VxLAN), and Fibre Channel over Ethernet (FCoE) network convergence.

Anytime

The *OmniSwitch AOS Release 8 CLI Reference Guide* contains comprehensive information on all CLI commands supported by the switch. This guide includes syntax, default, usage, example, related CLI command, and CLI-to-MIB variable mapping information for all CLI commands supported by the switch. This guide can be consulted anytime during the configuration process to find detailed and specific information on each CLI command.

Related Documentation

The following are the titles and descriptions of all the related OmniSwitch user manuals:

- *OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900 Hardware Users Guides*

  Describes the hardware and software procedures for getting an OmniSwitch up and running as well as complete technical specifications and procedures for all OmniSwitch chassis, power supplies, fans, and Network Interface (NI) modules.

- *OmniSwitch AOS Release 8 CLI Reference Guide*

  Complete reference to all CLI commands supported on the OmniSwitch. Includes syntax definitions, default values, examples, usage guidelines and CLI-to-MIB variable mappings.

- *OmniSwitch AOS Release 8 Switch Management Guide*

  Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, image rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

- *OmniSwitch AOS Release 8 Network Configuration Guide*

  Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols, such as RIP and IPX), security options (authenticated VLANs), Quality of Service (QoS), link aggregation, and server load balancing.

- *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide*

  Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package. Chapters cover multicast routing (DVMRP and PIM-SM), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).

- *OmniSwitch AOS Release 8 Data Center Switching Guide*

  Includes an introduction to the OmniSwitch data center switching architecture as well as network configuration procedures and descriptive information on all the software features and protocols that support this architecture. Chapters cover Data Center Bridging (DCB) protocols, Virtual Network Profile (vNP), VxLAN, and FCoE/FC transit and gateway functionality.

- *OmniSwitch AOS Release 8 Transceivers Guide*

  Includes SFP and XFP transceiver specifications and product compatibility information.

- *OmniSwitch AOS Release 8 Specifications Guide*

  Includes Specifications table information for the features documented in the Switch Management Guide, Network Configuration Guide, Advanced Routing Guide, and Data Center Switching Guide.

- Technical Tips, Field Notices

  Includes information published by Alcatel-Lucent Enterprise's Customer Support group.

- *Release Notes*

  Includes critical Open Problem Reports, feature exceptions, and other important information on the features supported in the current release and any limitations to their support.

Technical Support

An Alcatel-Lucent Enterprise service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel-Lucent Enterprise product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners.

With 24-hour access to Alcatel-Lucent Enterprise's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel-Lucent Enterprise's technical support, open a new case or access helpful release notes, technical bulletins, and manuals.

Access additional information on Alcatel-Lucent Enterprise's Service Programs:

Web: businessportal2.alcatel-lucent.com

Phone: 1-800-995-2696

Email: ebg_global_supportcenter@al-enterprise.com

1 Ethernet Port Commands

The Ethernet port software is responsible for configuring and monitoring Ethernet ports. This includes:

- Performing hardware diagnostics, loading software, and initializing hardware.
- Notifying other software modules in the system when Ethernet links become active or inactive.
- Configuring basic line parameters for Ethernet ports.
- Gathering basic line statistics for Ethernet ports and passing this information to the user interface and configuration manager.

MIB information for the Ethernet Port commands is as follows:

Filename: ALCATEL-IND1-PORT-MIB.mib
Module: alcatelIND1PortMIB

Filename: EtherLike-MIB.mib
Module: etherMIB

A summary of the available commands is listed here.

Interfaces commands	**interfaces** **interfaces speed** **interfaces crossover** **interfaces duplex** **interfaces alias** **clear interfaces** **interfaces max-frame-size** **interfaces inter-frame-gap** **interfaces flood-limit** **interfaces flood-limit action** **interfaces ingress-bandwidth** **interfaces pause** **interfaces link-trap** **interfaces ddm** **interfaces ddm-trap** **interfaces wait-to-restore** **interfaces wait-to-shutdown** **interfaces eee** **interfaces primary-port split-mode** **interfaces fec** **interfaces hybrid-mode** **interfaces loopback** **clear violation** **show interfaces** **show interfaces alias** **show interfaces status** **show interfaces capability** **show interfaces accounting** **show interfaces counters** **show interfaces counters errors** **show interfaces flood-rate** **show interfaces traffic** **show interfaces ingress-rate-limit** **show interfaces ddm** **show interfaces split-mode** **show transceivers** **show violation**
Interface violation commands	**violation recovery-maximum** **violation recovery-time** **violation recovery-trap** **show violation** **show violation-recovery-configuration** **clear violation**
Link monitoring commands	**interfaces link-monitoring admin-status** **interfaces link-monitoring time-window** **interfaces link-monitoring link-flap-threshold** **interfaces link-monitoring link-error-threshold** **interfaces clear-link-monitoring-stats** **show interfaces link-monitoring config** **show interfaces link-monitoring statistics**

Time Domain Reflectometry (TDR) commands	**interfaces tdr** **show interfaces tdr-statistics**
Link fault propagation commands	**link-fault-propagation group** **link-fault-propagation group source** **link-fault-propagation group destination** **link-fault-propagation group wait-to-shutdown** **show link-fault-propagation group**
LED beacon commands	**interfaces beacon** **show interfaces beacon**
IEEE 1588 Precision Time Protocol (PTP) commands	**interfaces ptp admin-state** **interfaces port ptp p2p** **show interfaces ptp config**
MAC Security commands	**interfaces macsec admin-state** **show interfaces macsec** **show interfaces macsec static** **show interfaces macsec dynamic** **show interfaces macsec statistics** **clear interfaces macsec statistics**

interfaces

Enables or disables auto negotiation or administrative status on a single port, a range of ports, or an entire Network Interface (NI).

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} {admin-state | autoneg | epp} {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
admin-state enable	Enables administrative state.
admin-state disable	Disables administrative state.
autoneg enable	Enables auto negotiation.
autoneg disable	Disables auto negotiation.
epp enable	Enables Enhanced Port Performance.
epp disable	Disables Enhanced Port Performance.

Defaults

parameter	default
enable | **disable**	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If auto negotiation is disabled, auto MDIX, flow control, auto speed, and auto duplex are not accepted. See the **interfaces crossover** command on page 1-8 and the **interfaces duplex** command on page 1-10 for more information.
- When EPP is enabled the fiber port receiver performance is enhanced by increasing its sampling rate. This enhancement can help with port link connection reliability or CRC problems that may occur with direct copper cable interfaces.
- Autonegotiation cannot be disabled on 10GBase-T ports.
- The 2.5G capable ports will advertise either 2.5G or 1G when auto-negotiation is enabled depending on the port's configured speed. The default is 2.5G.
- Autonegotiation is disabled for 10G port types and optical transceivers. It is enabled for 25G, 40G, and 100G direct-attached cables.

Examples

```
-> interfaces port 1/3/1 autoneg disable
-> interfaces slot 1/3 autoneg disable
-> interfaces port 1/3/1-4 autoneg disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces speed	Configures interface speed.
interfaces crossover	Configures crossover port settings.
interfaces duplex	Enables or disables flow (pause).
show interfaces alias	Displays interface line settings.
show interfaces	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgAutoNegotiation
```

interfaces speed

Configures interface line speed.

interfaces {slot *chassis/slot* | **port** *chassis/slot/port* **[-***port2***]} speed {10 | 100 | 1000 | 2500 | 10000 | 40000 | 100000 | 2000 | 4000 | 8000 | auto | max {100 | 1000 | 4000 | 8000}}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
auto	The switch automatically sets the line speed to match the attached device (auto-sensing).
10	Sets the interface to 10 Mbps.
100	Sets the interface to 100 Mbps.
1000	Sets the interface to 1000 Mbps (1 Gigabit).
2500	Sets the interface to 2500 Mbps (2.5 Gigabits).
10000	Sets the interface to 40000 Mbps (10 Gigabits).
40000	Sets the interface to 10000 Mbps (40 Gigabits).
100000	Sets the interface to 100000 Mbps (100 Gigabits).
2000	Sets the interface to 2000 Mbps for FibreChannel.
4000	Sets the interface to 4000 Mbps for FibreChannel.
8000	Sets the interface to 8000 Mbps for FibreChannel.
max 100	Sets the maximum speed to 100 Mpbs.
max 1000	Sets the maximum speed to 1000 Mbps (1 Gigabit).
max 4000	Sets the maximum speed to 4000 Mbps for FibreChannel.
max 8000	Sets the maximum speed to 8000 Mbps for FibreChannel.

Defaults

parameter	default
auto	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The changing of a port's speed, when changing between 100M/1G and 2.5G or vice-versa, is applied in port pairs. Meaning, changing the speed of one port of a pair will cause the other port's speed to change as well. The port pairs are 17/18, 19/20, 21/22, 23/24. This does not apply when changing the speed between 100M and 1G.

Examples

```
-> interfaces slot 1/3 speed auto
-> interfaces port 1/3/1 speed 100
-> interfaces port 1/3/2-8 speed 1000
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgSpeed
```

interfaces crossover

Configures port crossover settings on a single port, a range of ports, or an entire Network Interface (NI).

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} crossover {auto | mdix | mdi}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
auto	The interface automatically detects the crossover settings.
mdix	Sets the crossover configuration to Media Dependent Interface with Crossover (MDIX), which is the standard for hubs and switches.
mdi	Sets the crossover configuration to Media Dependent Interface (MDI), which is the standard for end stations.

Defaults

parameter	default
auto | mdix | mdi	**auto**

Platforms Supported

Not supported in this release.

Usage Guidelines

- If auto negotiation is disabled, then automatic crossover is also disabled. See the **interfaces** command for more information.
- You cannot configure crossover settings on fiber ports. These ports use the MDI standard.

Examples

```
-> interfaces slot 1/3 crossover mdi
-> interfaces port 1/3/1 crossover mdix
-> interfaces port 1/3/1-4 crossover auto
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgCrossover
```

interfaces duplex

Configures duplex mode. In full duplex mode, the interface transmits and receives data simultaneously. In half duplex mode, the interface can transmit *or* receive data at a given time. Auto duplex setting causes the switch to advertise all available duplex modes (half/full/both) for the port during autonegotiation.

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} duplex {full | half | auto}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
full	Sets interface to full duplex mode.
half	Sets interface to half duplex mode.
auto	Switch automatically sets both the duplex mode settings to auto-negotiation.

Defaults

parameter	default
full | half | auto	**full**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- The OmniSwitch OS6860(E)/6865/6900 do not support 10/100 half-duplex.
- Half duplex mode is not supported on Gigabit modules if a port is detected as Gigabit (1000 Mbps).
- Gigabit and 10 Gigabit fiber ports only support full duplex.

Examples

```
-> interfaces port 1/3/1 duplex auto
-> interfaces slot 1/3 duplex half
-> interfaces port 1/3/1-4 auto
```

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces	Configures interface line speed. Set to **auto** to set speed and duplex mode to auto-sensing.
show interfaces	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortAutoDuplexMode
```

interfaces alias

Configures a description (alias) for a single port.

interfaces port *chassis/slot/port* **alias** *description*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number.
description	A description for the port, which can be up to 64 characters long. Description tags with spaces must be enclosed within quotes (e.g., “IP Phone”).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You can only configure one port at time. You cannot configure an alias for multiple ports.
- To remove an alias use a description consisting of two quotes without any spaces (e.g., "").

Examples

```
-> interfaces port 1/3/1 alias "switch port"
-> interfaces port 1/2/2 alias "IP Phone"
-> interfaces port 1/3/1 alias ""
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces alias	Displays port status (up or down) and any aliases for a port.

MIB Objects

```
ifXTable
   ifAlias
```

clear interfaces

Resets all Layer 2 statistics counters or Time Domain Reflectometry (TDR) statistics counters.

clear interfaces {slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***] {l2-statistics [cli] | tdr-statistics}**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
cli	Clears the CLI statistics only.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- TDR is supported only on the OmniSwitch 6860.
- There is no global clear statistics command for TDR. The highest level granularity supported for clearing statistics is per *chassis/slot*.

Examples

```
-> clear interfaces port 1/1/20 l2-statistics
-> clear interfaces port 1/1/30 l2-statistics cli
-> clear interfaces port 1/1/40 tdr-statistics
```

Release History

Release 7.1.1; command introduced.
Release 8.1.1; **tdr-statistics** parameter added.

Related Commands

show interfaces counters	Displays general interface information, including when statistics were last cleared.
show interfaces tdr-statistics	Displays the results of the last TDR test performed on a port.

MIB Objects

```
alcetherStatsTable
   alcetherClearStats
esmTdrPortTable
   esmTdrPortClearResults
```

interfaces max-frame-size

Configures the maximum frame size for Gigabit Ethernet interfaces.

interfaces {slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***]} max-frame-size** *bytes*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
bytes	Maximum frame size, in bytes. Valid range is 1518–9216.

Defaults

parameter	default
bytes (Gigabit Ethernet Packets)	9216
bytes (Ethernet Packets)	1553

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> interfaces port 1/3/1 max-frame-size 1518
-> interfaces slot 1/3 max-frame-size 1518
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgMaxFrameSize
```

interfaces inter-frame-gap

Configures the inter-frame gap.

interfaces {slot *chassis/slot* | **port** *chassis/slot/port***[**-*port2*]} **inter-frame-gap** *bytes*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2*]	The port number. Use a hyphen to specify a range of ports.
bytes	Number of bytes for the inter-frame gap. Valid range is 8-31 bytes.

Defaults

parameter	default
bytes	12

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> interfaces port 1/1/1 inter-frame-gap 15
```

Release History

Release 8.4.1.R01; command was introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

N/A

interfaces flood-limit

Configures the flood rate settings on a single port, a range of ports, or an entire Network Interface (NI).

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[-***port2***]} flood-limit {bcast | mcast | uucast | all} rate {pps** *pps_num*| **mbps** *mbps_num* **| cap%** *cap_num* **| enable | disable | default} [low-threshold** *low_num***]**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
bcast	Specifies broadcast flood limit.
mcast	Specifies multicast flood limit.
uucast	Specifies unicast flood limit.
all	Specifies flood limit for all types of traffic.
pps_num	Packets per second.
mbps_num	Megabits per second.
cap_num	Percentage of port's capacity.
enable	Enables flood rate limits.
disable	Disables flood rate limits.
default	Sets default flood rate limits
low_num	Specifies the low threshold value, which must be lower than the high threshold value set for the *pps_num*, *mbps_num*, or *cap_num* value.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The packets-per-second (**pps**) setting is based on a 512 byte frame size. When configuring the threshold value as a percentage (**cap%**) or in megabits-per-second (**mbps**), only approximate limits can be achieved because values are always estimated based on the packet-per-second size (512 bytes).
- The **low-threshold** parameter is set to help with the auto-recovery of a port that was shutdown because of a STORM violated state. The shutdown action is configured through the **interfaces flood-limit action** command.

Examples

```
-> interfaces slot 1/2 flood-limit all rate cap% 50
-> interfaces slot 1/3 flood-limit bcast rate mbps 100
-> interfaces port 1/1/1 flood-limit bcast rate mbps 60 low-threshold 40
-> interfaces port 1/1/5 flood-limit mcast rate pps 2000 low-threshold 1000
```

Release History

Release 7.1.1; command introduced.
Release 8.2.1; **default** and **low-threshold** parameters added.

Related Commands

show interfaces flood-rate	Displays interface flood rate settings.

MIB Objects

```
esmConfigTable
   esmPortCfgFlow
dot3PauseTable
   dot3PauseAdminMode
```

interfaces flood-limit action

Configures the action on a single port, a range of ports, when the port reaches the storm violated state.

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[-***port2***]} flood-limit {bcast | mcast | uucast | all} action {shutdown | trap | default}**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to configure.
port	Port number of the interface to configure.
port2	Last port number in a range of ports to configure.
bcast	Broadcast flood limit.
mcast	Multicast flood limit.
uucast	Unicast flood limit.
all	Flood limit for all types of traffic.
shutdown	When the high threshold is violated, port is put into a blocked state.
trap	When the high threshold is crossed, trap is sent with the violation reason.
default	When traffic reaches the high threshold, packets above that rate will be dropped.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When high threshold is violated, and the port needs to be put in blocked state, set the action as "**shutdown**".
- Use the **low-threshold** parameter of the **interfaces flood-limit** command to assist with auto-recovery of a port that was shutdown.
- When high threshold is crossed, and a trap has to be sent with violation reason, set the action as "**trap**".
- When traffic reaches high threshold, and the packets above that rate needs to be dropped, set the action as "**default**".

Examples

```
-> interfaces port 1/1/1 flood-limit bcast action shutdown
-> interfaces port 1/1/4 flood uucast action trap
-> interfaces port 1/1/11 flood-limit all action shutdown
-> interfaces port 1/1/14 flood mcast action default
```

Release History

Release 8.2.1; command introduced.

Related Commands

interfaces flood-limit	Configures the high and low threshold values for flood rate limiting.
show interfaces flood-rate	Displays interface flood rate settings.

MIB Objects

```
esmConfigTable
   esmPortBcastThresholdAction
   esmPortMcastThresholdAction
   esmPortUucastThresholdAction
```

interfaces ingress-bandwidth

Configures the ingress bandwidth settings on a single port, a range of ports, or an entire Network Interface (NI).

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} ingress-bandwidth {mbps| enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
mbps	Specifies the ingress bandwidth in mbps.
enable	Enables ingress bandwidth limiting.
disable	Disables ingress bandwidth limiting.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> interfaces slot 1/3 ingress-bandwidth enable
-> interfaces slot 1/3 ingress-bandwidth mbps 30
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces ingress-rate-limit	Displays the ingress-rate-limit set for each interface port.

MIB Objects

```
esmConfTable
   esmPortIngressRateLimitEnable
```

interfaces pause

Configures whether or not the switch will transmit and/or honor flow control PAUSE frames on the specified interface. PAUSE frames are used to temporarily pause the flow of traffic between two connected devices to help prevent packet loss when traffic congestion occurs between switches.

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} pause {tx | rx | tx-and-rx | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
tx	Allows interface to transmit PAUSE frames to peer switches.
rx	Allows interface to honor PAUSE frames from peer switches and temporarily stop sending traffic to the peer.
tx-and-rx	Allows the interface to transmit and honor PAUSE frames to/from peer switches.
disable	Disables flow control on the interface.

Defaults

By default, flow control is disabled on all switch interfaces.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Flow control is only supported on interfaces configured to run in full-duplex mode; half-duplex mode is not supported. In addition, flow control is not supported across a virtual fabric link (VFL).
- If both autonegotiation and flow control are enabled on the same local interface, autonegotiation calculates operational flow control settings for that interface. Note that the operational settings override the configured settings as long as autonegotiation and flow control are both enabled for the interface.
- If autonegotiation is disabled, the configured flow control settings are applied to the local interface.

Examples

```
-> interfaces port 1/2/4 pause rx
-> interfaces port 1/1/11 pause tx
-> interfaces port 1/2/1 pause tx-and-rx
-> interfaces port 1/2/1-6 disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces status	Displays interface line settings.

MIB Objects

```
esmConfTable
   esmPortCfgPause
```

interfaces link-trap

Enables trap link messages. If enabled, a trap is generated whenever the port changes state.

interfaces [slot *chassis/slot* | **port** *chassis/slot/port* **[**-*port2***]] link-trap {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
enable	Port link up/down traps are displayed on the NMS.
disable	Port link up/down traps are not displayed on the NMS.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> interfaces port 1/2/1 link-trap enable
-> interfaces slot 1/3 link-trap enable
-> interfaces port 1/1/1-6 link-trap enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces status	Displays interface line settings.

MIB Objects

```
esmConfigTable
   esmPortSlot
   esmPortIF
```

interfaces ddm

Configures the Digital Diagnostics Monitoring (DDM) administrative status.

interfaces ddm {enable | disable}

Syntax Definitions

enable	Enables DDM functionality.
disable	Disables DDM functionality.

Defaults

parameter	default
ddm	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- DDM capability will vary based on the transceiver manufacturer.
- DDM status must be enabled in order to enable traps; traps are enabled separately.

Examples

```
-> interfaces ddm enable
-> interfaces ddm disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces ddm	Displays the interface DDM status.

MIB Objects

```
ddmConfiguration
   ddmConfig
```

interfaces ddm-trap

Configures the Digital Diagnostics Monitoring (DDM) administrative status or trap capability.

interfaces ddm-trap {enable | disable}

Syntax Definitions

enable	Enables DDM trap functionality.
disable	Disables DDM trap functionality.

Defaults

parameter	default
ddm-trap	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

DDM status must be enabled in order to enable traps; traps are enabled separately.

Examples

```
-> interfaces ddm-trap enable
-> interfaces ddm-trap disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces ddm	Displays the interface DDM status.

MIB Objects

```
ddmConfiguration
   ddmTrapConfig
   ddmNotificationType
```

interfaces wait-to-restore

Configures the wait to restore timer on a specific slot, port, or a range of specified ports. The timer is enabled when a link up event is detected. Other applications are notified of the link up event only after the wait to restore timer has elapsed.

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} wait-to-restore** *num*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
num	The number of seconds the switch waits before notifying other applications. The valid range is 0-300 in multiples of 5 seconds.

Defaults

By default, the timer is set to zero (disabled).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Set the wait-to-restore timer to zero to disable the timer.
- Enter a slot number to configure the timer value for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the timer value for a specific interface or a range of interfaces.

Example

```
-> interfaces slot 1/1 wait-to-restore 30
-> interfaces port 1/1/1 wait-to-restore 10
-> interfaces port 1/1/1-7 wait-to-restore 250
```

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonWaitToRestoreTimer
```

interfaces wait-to-shutdown

Configures the wait to shutdown timer on a specific slot, port, or a range of specified ports. The timer is enabled when a link down event is detected. Other applications are notified of the link down event only after the wait to shutdown timer has elapsed.

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} wait-to-shutdown** *num*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
num	The number of milliseconds the switch waits before notifying other applications. The valid range is 0-300 in multiples of 10msec.

Defaults

By default, the timer is set to zero (disabled).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command can be used to reduce port flapping. If the port comes back up before the timer expires then the timer will be canceled and other applications will not be notified of the link down event.
- Set the wait-to-shutdown timer to zero to disable the timer.
- The WTS timer is not started when the switch is first booted. But administratively disabling the port will start the timer if enabled.
- The link-status of the remote port will be down when the WTS timer is running. This is due to the port being physically down and only the link-down event not being communicated to other applications.

Example

```
-> interfaces slot 1/1 wait-to-shutdown 30
-> interfaces port 1/1/1 wait-to-shutdown 10
-> interfaces port 1/1/1-7 wait-to-shutdown 250
```

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonWaittoShutdownTimer
```

interfaces eee

Enables or disabled Energy Efficient Ethernet.

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} eee {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
enable	Enables EEE functionality.
disable	Disables EEE functionality.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- EEE is only supported on copper ports.
- Enabling EEE will start advertising EEE capability to peer ports. Disabling EEE will stop advertising EEE capability to peer ports.

Examples

```
-> interfaces port 1/1/1 eee enable
-> interfaces slot 1/1 eee disable
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

N/A

interfaces primary-port split-mode

Configures the mode of splitter cable capable ports.

interfaces primary-port *chassis/slot/port* **split-mode {auto | 4X25G | 4X10G | 40G | 100G}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
port	The port number.
auto	Automatically detects if a splitter cable is connected.
4x10g	Sets the port to the 4X10G splitter functionality.
4x25g	Sets the port to the 4X25G splitter functionality.
40g	Sets the port to 40G functionality.
100g	Sets the port to 100G functionality.

Defaults

parameter	default
enable | disable	**auto**

Platforms Supported

OmniSwitch 6900, 9900

Usage Guidelines

- This command is only supported on ports and platforms that support the splitter cable functionality.
- The proper cable should be used based on the port's configuration. For example, if set to 4X10G with a 40G cable connected, the port will only operate as a 10G port.

Examples

```
-> interfaces primary-port 1/1/1 split-mode 4X10G
```

Release History

Release 7.3.4; command was introduced.
Release 8.5R2; **primary-port** keyword added.

Related Commands

show interfaces split-mode	Displays the configured and operational state of the splitter cable capable ports.

MIB Objects

```
esmPortModeTable
  esmConfiguredMode
```

interfaces fec

Configures the Reed Solomon (RS-FEC) and Fire Code (FC-FEC) FEC also known as BASE-R FEC.

interfaces {slot *chassis/slot* | **port** *chassis/slot/port***[**-*port2*]} **fec {disable | auto | fc | rs}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2*]	The port number. Use a hyphen to specify a range of ports.
disable	Disables FEC.
auto	Automatically determines the FEC.
fc	FC-FEC is forced.
rs	RS-FEC is forced.

Defaults

parameter	default
fec	auto

Platforms Supported

OmniSwitch 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- This command is only supported on modules that support FEC configuration.
- For 10G/40G the FEC will default to FC-FEC. For 25G/100G the FEC will default to RS-FEC.

Examples

```
-> interfaces port 1/1/1 fec fc
-> interfaces slot 1/2 fec auto
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

show interfaces status	Displays the configured and operational state of the ports.

MIB Objects

```
esmPortModeTable
  esmConfiguredMode
```

interfaces hybrid-mode

Configures the mode of a combo port to either fiber or copper.

interfaces {slot *chassis/slot* | **port** *chassis/slot/port***[**-*port2***]} hybrid-mode {fiber | copper}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
fiber	Enables the fiber combo port.
copper	Enables the copper combo port.

Defaults

parameter	default
hybrid-mode	fiber
Fiber/Copper Speed	1000Mbps/auto
Fiber/Copper Duplex	Full/auto
Fiber/Copper Autoneg	Enabled/Enabled

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Each combo port can be set to either fiber or copper but not both at the same time.
- When the mode is changed on a port the speed, duplex and auto-negotiation parameters will be set to the default for that port type (see table above). Other port settings will remain the same (i.e. admin status, flood limits, alias, etc.)

Examples

```
-> interfaces port 1/1/9 hybrid-mode copper
-> interfaces port 1/1/10 hybrid-mode fiber
```

Release History

Release 8.6R1; command introduced.

Related Commands

interfaces speed	Configures interface speed.
interfaces crossover	Configures crossover port settings.
interfaces duplex	Enables or disables flow (pause).
show interfaces status	Displays interface line settings.
show interfaces	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgHybridActiveType
   esmPortCfgHybridMode
   esmPortOperationalHybridType
```

interfaces loopback

Enables or disables the loopback mode for the specified front-panel port. Enable the port loopback mode to support L3 VPN inline routing for an IP over Shortest Path Bridging (SPB) configuration.

interfaces port *chassis/slot/port***[**-*port2***] loopback**

no interfaces port *chassis/slot/port***[**-*port2***] loopback**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.

Defaults

By default, the port loopback mode is disabled.

Platforms Supported

OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to disable the port loopback mode.
- This command applies only to front-panel ports. A single port can provide the loopback function or the port can be assigned to a static link aggregate that is also configured to run in loopback mode.
- When the loopback mode is enabled, the port can be configured as a bridge and access port to provide the loopback functionality on the same port (no external cable required). However, other switch functionality is not supported on loopback ports.
- For more information about SPB L3 VPN, see the “IP over SPBM” section of the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide.*

Examples

```
-> interfaces port 1/1/1 loopback
-> interfaces port 1/1/2-5 loopback
-> no interfaces port 1/1/1 loopback
```

Release History

Release 8.6R2; command introduced.

Related Commands

linkagg static agg loopback	Configures a link aggregate to run in the loopback mode.
show interfaces status	Displays the interface line settings (for example, speed and mode).
show interfaces	Displays general interface information (for example, hardware, MAC address, input errors, and output errors).

MIB Objects

```
alaPortXTable
   alaPortXLoopbackStatus
```

clear violation

Clears all the MAC address violation logs for a particular port and session. After the violations are cleared, the specific port resumes normal operation. This includes applying an existing application configuration.

clear violation {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
*agg_id***[**-*agg_id2***]**	Enter a link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When a violation is set on a physical port that is part of a link aggregate, the violation is set for the whole link aggregate. All ports on that link aggregate are brought down. When this command is applied to a link aggregate ID, all member ports of the link aggregate are activated.
- When this command is applied, all MAC addresses known to the port are cleared from the MAC address table for the switch.

Examples

```
-> clear violation port 1/10
-> clear violation port 2/1-5
-> clear violation linkagg 5
-> clear violation linkagg 10-20
```

Release History

Release 7.1.1; command introduced.

Related Commands

show violation	Displays the address violations that occur on ports with LPS restrictions.

MIB Objects

```
portViolationTable
   portViolationClearPort
```

violation recovery-maximum

Configures the maximum number of recovery attempts allowed before the port is permanently shut down. This value is configurable on a global basis (applies to all ports on all modules) and on a per-slot or per-port basis.

violation recovery-maximum {infinite | *max_attempts***}**

violation [slot *chassis/slot* **| port** *chassis/slot/port***[-***port2***]] recovery-maximum {infinite | default |** *max_attempts***}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
infinite	Sets the recovery attempt to infinite auto recovery.
default	Sets the number of recovery attempts to the global value for the specified ports. This parameter is only available when a slot, port, or range of ports is specified with this command.
max_attempts	The maximum number of recovery attempts. Valid range is 0-50.

Defaults

By default, this command configures the global maximum number of recovery attempts. The global value applies to all ports on all modules in the switch.

parameter	default
max_attempts	10

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Set the maximum number of recovery attempts value to 0 to disable this recovery mechanism.
- Enter a slot number to configure the number of recovery attempts for all interfaces on a specific slot.
- Enter a slot and port number or a range of ports to configure the number of recovery attempts for a specific interface or a range of interfaces.
- When this command is used to configure the number of recovery attempts for all ports on a slot or for a specific port or range of ports, the value specified overrides the global maximum number of attempts configured for the switch.
- When configuring the number of recovery attempts for a specific slot, port, or range of ports, use the **default** parameter to reset this value to the global maximum number of attempts.

- The number of recovery attempts increments whenever a port recovers using automatic recovery timer mechanism. When the number of recovery attempts exceeds the configured threshold, the port is permanently shut down.
- Once an interface is permanently shut down, only the **clear violation** command can be used to recover the interface.
- The recovery mechanism tracks the number of recoveries within a fixed time window (FTW). The FTW = 2 * maximum recovery number * recovery timer. For example, if the maximum number of recovery attempts is set to 4 and the recovery timer is set to 5, the FTW is 40 seconds (2 * 4 * 5=40).

Examples

```
-> violation recovery-maximum 25
-> violation slot 1/2 recovery-maximum 10
-> violation port 1/2/3 recovery-maximum 20
-> violation port 1/2/4-9 recovery-maximum 50
-> violation port 1/2/4-9 recovery-maximum default
-> violation port 1/2/3 recovery-maximum 0
-> violation recovery-maximum infinite
-> violation recovery-maximum 0
```

Release History

Release 8.2.1; command was introduced.

Related Commands

violation recovery-time	Configures the time interval after which the port is automatically re-activated if the port was shut down for any violation.
show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show violation-recovery-configuration	Displays the globally configured recovery time, SNMP recovery trap status, and maximum recovery attempts.

MIB Objects

```
alaPortViolationRecoveryTable
   alaPortViolationRecoveryMaximum
```

violation recovery-time

Configures the time interval after which the port is automatically re-activated if the port was shutdown for any violation. This value is configurable on a global basis (applies to all ports on all modules) and on a per-slot or per-port basis.

violation recovery-time *seconds*

violation [slot *chassis/slot* **| port** *chassis/slot/port***[**-*port2***]] recovery-time {***seconds* | **default}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of port.
seconds	The number of seconds after which a port is reactivated. The valid range is 30-600 seconds.
default	Sets the recovery time to the global value for the specified ports. This parameter is only available when a slot, port, or range of ports is specified with this command.

Defaults

- By default, this command configures the global recovery time. The global value applies to all ports on all modules in the switch.
- By default, the violation recovery time is set to 300 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- When the recovery timer expires, the interface is operationally re-enabled and the violation on the interface is cleared.
- The violation recovery time value does not apply to interfaces that are in a permanent shutdown state. A port in this state is only recoverable using the **clear violation** command.
- The interface violation recovery mechanism is not supported on link aggregates, but is supported on the link aggregate member ports.
- Enter a slot number to configure the recovery time for all interfaces on a specific slot.
- Enter a slot and port number or a range of ports to configure the recovery time for a specific interface or a range of interfaces.
- When this command is used to configure the recovery time for all ports on a slot or for a specific port or range of ports, the value specified overrides the global maximum recovery time configured for the switch.

- When configuring the time for a specific slot, port, or range of ports, use the **default** parameter to reset this value to the global maximum number of attempts.

Examples

```
-> violation recovery-time 600
-> violation slot 1/2 recovery-time 100
-> violation port 1/2/3 recovery-time 200
-> violation port 1/2/4-9 recovery-time 500
-> violation port 1/2/4-9 recovery-time default
```

Release History

Release 8.2.1; command introduced.

Related Commands

violation recovery-maximum	Configures the maximum number of recovery attempts before a port is permanently shut down.
show violation	Displays the violation and recovery status for the specified port.
show violation-recovery-configuration	Displays the globally configured recovery time, SNMP recovery trap enable/disable status and maximum recovery attempts.

MIB Objects

```
alaPortViolationRecoveryTable
   alaPortViolationRecoveryTime
```

violation recovery-trap

Enables or disables the sending of a violation recovery trap when any port is re-enabled after the violation recovery time has expired.

violation recovery-trap {enable | disable}

Syntax Definitions

enable	Enables the ports to send violation recovery traps.
disable	Disables the ports from sending violation recovery traps.

Defaults

By default, sending of a violation recovery trap is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

This is a global command that is applied to all ports on all modules.

Examples

```
-> violation recovery-trap enable
-> violation recovery-trap disable
```

Release History

Release 8.2.1; command was introduced.

Related Commands

violation recovery-time	Configures the time interval to automatically re-enable the ports that were shutdown due to a violation.
show violation-recovery-configuration	Displays the globally configured recovery time, SNMP recovery trap status, and maximum recovery attempts.

MIB Objects

```
esmViolationRecovery
   esmViolationRecoveryTrap
```

show interfaces

Displays general interface information (for example, hardware, MAC address, input errors, and output errors).

show interfaces [slot *chassis/slot* | **port** *chassis/*slot/*port***[-***port2***]]**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The Link-Quality parameter and Enhanced Port Performance capabilities are only supported on the OmniSwitch 6900.
- EEE will be appended to the Autonegotiation output when EEE is enabled (EEE is supported only on the OmniSwitch 6860, 6865, 6900).

Examples

```
-> show interfaces port 1/1/2
Chassis/Slot/Port 1/1/2  :
  Operational Status     : up,
  Last Time Link Changed : Mon Jan  5 17:09:30 2019,
  Number of Status Change: 1,
  Port-Down/Violation Reason: None,
  Type                   : Ethernet,
  SFP/XFP                : GBIC_SX,
  Interface Type         : Fiber,
  EPP                    : Disabled,
  Link-Quality           : Good
  MAC address            : 00:d0:95:b2:39:85,
  BandWidth (Megabits)   : 1000,                Duplex           : Full,
  Autonegotiation        :   1  [ 1000-F 100-F 100-H 10-F 10-H ],
  Long Accept            : Enable,              Runt Accept      : Disable,
  Long Frame Size(Bytes) : 9216,                Runt Size(Bytes) : 64,
  Inter Frame Gap(Bytes) : 12,
  loopback mode          : N/A,
  Rx             :
  Bytes Received  :             7967624, Unicast Frames :                  0,
  Broadcast Frames:              124186, M-cast Frames  :                290,
```

```
UnderSize Frames:                   0, OverSize Frames:                   0,
Lost Frames     :                   0, Error Frames   :                   0,
CRC Error Frames:                   0, Alignments Err :                   0,
Tx              :
Bytes Xmitted   :           255804426, Unicast Frames :               24992,
Broadcast Frames:             3178399, M-cast Frames  :              465789,
UnderSize Frames:                   0, OverSize Frames:                   0,
Lost Frames     :                   0, Collided Frames:                   0,
```

output definitions

Slot/Port	Interface slot and port.
Operational Status	Interface status: up - port is operationally up. down - port is operationally down dormant - SFP/SFP+ transceiver is inserted into a port configured for Fibre Channel or Fibre Channel transceiver in inserted into a port configured for Ethernet and the link has become active.
Last Time Link Changed	The last time the configuration for this interface was changed.
Number of Status Change	The total number of times that the configuration of this interface has changed.
Port-Down/Violation Reason	This is displayed if the port is down. If the port is down due to software reasons or violations the reason is displayed. If it is down due to physical fault, “None” is displayed. The reason displayed applies only to the physical port, for a link aggregate use the **show violation** command.
Type	Interface type (Ethernet/Fast Ethernet/Gigabit Ethernet).
SFP/XFP	The type of transceiver detected.
Interface Type	The type of interface for this port. (Copper, Fiber, Combo-Copper, Combo-Fiber)
EPP	Enhanced Port Performance setting.
Link-Quality	The link quality of the connection: **GOOD** - The port will connect with no problems and transfer data with no errors. **FAIR** - The port may have intermittent problems connecting and maintaining its connection to a remote port and/or intermittent CRC's could occur. **POOR** - The port will have problems connecting and maintaining a connection with remote port. If the ports connect, it’s likely CRC errors will occur. **N/A** - The port link quality is either very poor or the port type does not support the Link Quality capability.
MAC address	Interface MAC address.
WWPN	OmniSwitch 64-bit World Wide Port Name (WWPN) for each Fibre Channel port.
Bandwidth	Bandwidth (in megabits).
Duplex	Duplex mode (Half/Full/Auto).
Autonegotiation	The auto negotiation settings for this interface.

output definitions (continued)

Long Accept	Long Frames status (enable/disable).
Runt Accept	Runt Frames status (enable/disable).
Long Frame Size	Long Frame Size (in Bytes).
Runt Size	Runt Frame Size (in Bytes).
Inter Frame Gap	Inter-packet gap (in Bytes).
loopback mode	The loopback mode for the port (**N/A** or **SPB-VPN**). Ports are configured to run in the loopback mode to support L3 VPN inline routing for an IP over Shortest Path Bridging (SPB) configuration.
Bytes Received	Number of Bytes received.
Rx Unicast Frames	Number of unicast frames received.
Rx Broadcast Frames	Number of broadcast frames received.
Rx M-cast Frames	Number of multicast frames received.
Rx Undersize Frames	Number of undersized frames received.
Rx Oversize Frames	Number of oversized frames received.
Rx Lost Frames	Number of Lost Frames received.
Rx Error Frames	Number of error frames received.
Rx CRC Error Frames	Number of CRC error frames received. Only applies to frames that are less than or equal to Max/Long Frame Size. Frames larger than Long Frame Size are counted as OverSizeFrames.
Rx Alignments Err	Number of Alignments Error frames received.
Bytes Xmitted	Number of Bytes transmitted.
Tx Unicast Frames	Number of unicast frames transmitted.
Tx Broadcast Frames	Number of broadcast frames transmitted.
Tx M-cast Frames	Number of multicast frames r transmitted.
Tx Undersize Frames	Number of undersized frames transmitted.
Tx Oversize Frames	Number of oversized frames transmitted.
Tx Lost Frames	Number of Lost Frames transmitted.
Tx Collided Frames	Number of collision frames received or transmitted.
Tx Error Frames	Number of error frames transmitted.

Release History

Release 7.1.1; command introduced.
Release 8.6R2; “Port-Down Reason/Violation Reason”, “Interface Type”, and “loopback mode” output fields added.

Related Commands

show interfaces accounting	Displays interface accounting information (e.g., packets received/ transmitted).
show interfaces counters	Displays interface counter information (e.g., unicast packets received/transmitted).
show interfaces status	Displays the interface line settings (e.g., speed and mode).
show interfaces traffic	Displays interface traffic statistics (input/output bytes and packets).

MIB Objects

```
ifTable
   ifOperStatus
   ifType
   ifPhysAddress
   ifSpeed
   ifInDiscards
   IfOutDiscards
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortCfgLongEnable
   esmPortCfgRuntEnable
   esmPortCfgMaxFrameSize
   esmPortCfgRuntSize
   esmPortDownReason
   esmPortInterfaceType
alaPortXTable
   alaPortXLoopbackStatus
ifXTable
   ifHCInOctets
   ifHCInUcastPkts
   ifHCInBroadcastPkts
   ifHCInMulticastPkts
   IfHCOutOctets
   IfHCOutUcastPkts
   IfHCOutBroadcastPkts
   IfHCOutMulticastPkts
alcetherStatsTable
   alcetherStatsRxUndersizePkts
   alcetherStatsCRCAlignErrors
   alcetherStatsTxUndersizePkts
   alcetherStatsTxOversizePkts
   alcetherStatsTxCollisions
dot3StatsTable
   dot3StatsFrameTooLong
   dot3StatsFCSErrors
   dot3StatsLateCollisions
```

show interfaces alias

Displays interface line settings (e.g., speed and mode).

show interfaces [slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***]] alias**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If no slot/port numbers are entered, line settings for all slots/ports on the switch are displayed.

Examples

```
-> show interfaces port 1/1/2 alias
Legends:WTS - Wait to shutdown
# - WTS Timer is Running & port is in wait-to-shutdown state
Chas/
Slot/    Admin     Link    WTR   WTS   Alias
Port     Status   Status   (sec) (msec)
-----+----------+---------+-----+----+---------------------------------
1/1/2   disable    down    5     #10  ""
```

output definitions

Chas/Slot/Port	Interface chassis/slot/port number.
Admin Status	The administrative status of the port.
Link Status	The link status of the port.Autonegotiation status (Enable/Disable).
WTS (msec)	The wait-to-shutdown configuration time.
WTR (sec)	The wait-to-restore configuration time.
Alias	The configured alias for the port.

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces alias	Configures the port alias.

MIB Objects

```
ifXTable
   ifAlias
```

show interfaces status

Displays interface line settings (for example, speed and mode).

show interfaces [slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***]] status**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If no slot/port numbers are entered, line settings for all slots/ports on the switch are displayed.

Examples

```
-> show interfaces status
 Chas/                DETECTED-VALUES              CONFIGURED-VALUES
 Slot/   Admin  Auto  Speed   Duplex  Pause  FEC   Speed   Duplex  Pause  FEC   Link
 Port    Status Nego  (Mbps)                Det   (Mbps)                 Cfg   Trap  EEE
--------+------+----+--------+------+-------+----+--------+------+-------+-----+-----+---
 1/1/1A     en    en     -      -       -    -     40000    Full     -    AUTO  en   dis
 1/1/1B     en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/1/1C     en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/1/1D     en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/1/2A     en    en     -      -       -    -     40000    Full     -    AUTO  en   dis
 1/1/2B     en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/1/2C     en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/1/2D     en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/3/1      en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/3/2      en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/3/3      en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/3/4      en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
 1/3/5      en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis

-> show interfaces port 1/3/1 status
 Chas/                DETECTED-VALUES              CONFIGURED-VALUES
 Slot/   Admin  Auto  Speed   Duplex  Pause  FEC   Speed   Duplex  Pause  FEC   Link
 Port    Status Nego  (Mbps)                Det   (Mbps)                 Cfg   Trap  EEE
--------+------+----+--------+------+-------+----+--------+------+-------+-----+-----+---
 1/3/1      en   dis     -      -       -    -     10000    Full     -    AUTO  en   dis
```

output definitions

Chas/Slot/Port	Interface chassis/slot/port number.
Admin Status	The administrative status of the port. Configured through the **interfaces** command.
AutoNego	Autonegotiation status (Enable/Disable). Configured through the **interfaces** command.
Detected Speed	Detected line speed in Mbps.
Detected Duplex	Detected line duplex (Half duplex/Full duplex/Auto).
Detected Pause	Detected pause control configuration.
FEC Det	The detected FEC settings (DIS, FC, RS).
Configured Speed	Configured line speed (10/100/Auto/1000/10000 Mbps). Configured through the **interfaces speed** command.
Configured Duplex	Configured line duplex (Half duplex/Full duplex/Auto). Configured through the **interfaces duplex** command.
FEC Cfg	The configured FEC settings (Disable, Auto, FC, RS).
Configured Pause	Detected pause control configuration. Configured through the **interfaces pause** command.
Link Trap	Link Trap status. Configured through the **interfaces link-trap** command.
EEE	Energy Efficient Ethernet configuration (dis/ena).

Release History

Release 7.1.1; command introduced.
Release 8.4.1.R03; **FEC Det** and **FEC Cfg** fields added.

Related Commands

interfaces	Configures interface line speed, sets speed, and duplex mode to auto-sensing.
interfaces duplex	Configures interface duplex mode.
interfaces fec	Configures the Reed Solomon (RS-FEC) and Fire Code (FC-FEC) FEC also known as BASE-R FEC.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortAutoSpeed
   esmPortAutoDuplexMode
   esmPortCfgAutoNegotiation
   esmPortCfgSpeed
   esmPortCfgDuplexMode
   esmPortCfgPause
   esmPortLinkUpDownTrapEnable
```

show interfaces capability

Displays default auto negotiation, speed, duplex, flow, and cross-over settings for a single port, a range of ports, or all ports on a Network Interface (NI) module.

show interfaces [slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***]] capability**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Displays defaults settings in two rows of data for each port. The first row of data, identified by the label **CAP**, displays the valid user-defined configuration settings available for the port. The second row, identified by the label **DEF**, displays the default settings for the port.

Examples

```
-> show interfaces capability
                                                                          Macsec
Ch/Slot/Port   AutoNeg       Pause       Crossover     Speed    Duplex     Supported
--------------+--------+---------------+-----------+----------+----------+-----------
1/1/1   CAP   EN/DIS   Tx/Rx/Tx&Rx/DIS  MDI/X/Auto  10/100/1G  Full/Half    NO
1/1/1   DEF       EN               DIS        Auto       Auto       Auto
1/1/2   CAP   EN/DIS   Tx/Rx/Tx&Rx/DIS  MDI/X/Auto  10/100/1G  Full/Half    NO
1/1/2   DEF       EN               DIS        Auto       Auto       Auto
1/1/3   CAP   EN/DIS   Tx/Rx/Tx&Rx/DIS  MDI/X/Auto  10/100/1G  Full/Half    NO
1/1/3   DEF       EN               DIS        Auto       Auto       Auto
1/1/25  CAP      DIS   Tx/Rx/Tx&Rx/DIS           -        10G       Full    YES
1/1/25  DEF      DIS               DIS           -        10G       Full
1/1/26  CAP      DIS   Tx/Rx/Tx&Rx/DIS           -        10G       Full    YES
1/1/26  DEF      DIS               DIS           -        10G       Full

-> show interfaces port 1/1/1 capability
                                                                          Macsec
Ch/Slot/Port   AutoNeg       Pause       Crossover     Speed    Duplex     Supported
--------------+--------+---------------+-----------+----------+----------+-----------
1/1/1   CAP   EN/DIS   Tx/Rx/Tx&Rx/DIS  MDI/X/Auto  10/100/1G  Full/Half    NO
1/1/1   DEF       EN               DIS        Auto       Auto       Auto
```

output definitions

Cha/Slot/Port	The chassis/slot/port identifier.
AutoNeg	In the row labeled **CAP,** the field displays the valid auto negotiation configurations for the port. In the row label **DEF,** the field displays the default auto negotiation settings for the port. The possible values are **EN** (enabled) or **DIS** (disabled).
Pause	In the row labeled **CAP,** the field displays the valid pause configurations for the port. In the row label **DEF,** the field displays the default pause settings for the port.
Crossover	In the row labeled **CAP,** the field displays the valid cross over configurations for the port. In the row label **DEF,** the field displays the default cross over settings for the port. The possible values are **Auto**, **MDI/X/Auto** (MDI/MDIX/Auto), or **--** (not configurable and/or not applicable).
Speed	In the row labeled **CAP,** the field displays the valid line speed configurations for the port. In the row label **DEF,** the field displays the default line speed settings for the port. The possible values are **10/100**, **100**, **1G**, **10/100/1G**, **10G**, or **Auto**.
Duplex	In the row labeled **CAP,** the field displays the valid duplex configurations for the port. In the row label **DEF,** the field displays the default duplex settings for the port. The possible values are **Full**, **Full/Half**, or **Auto**.
Macsec Supported	The status of MACsec on the interface.

Release History

Release 7.1.1; command introduced.
Release 8.5 R1; **Macsec Supported** field added.

Related Commands

interfaces	Enables and disables auto negotiation.
interfaces crossover	Configures crossover port settings.
interfaces	Configures interface speed.
interfaces duplex	Configures duplex settings.
show interfaces alias	Displays interface line settings.

MIB Objects

```
esmConfTable
   esmPortCfgAutoNegotiation
   esmPortCfgFlow
   esmPortCfgCrossover
   esmPortCfgSpeed
   esmPortAutoDuplexMode
```

show interfaces accounting

Displays interface accounting information (e.g., packets received/transmitted and deferred frames received).

show interfaces [slot *chassis/slot* **| port** *chassis/slot/port***[-***port2***]] accounting**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*slot/port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If no slot/port numbers are entered, accounting information for all slots/ports on the switch is displayed.
- The OmniSwitch 9900 supports different packet size ranges than the other OmniSwitch platforms. All packets sized 1024 octets or larger are classified into the “1024 to MAX” category. As a result, this command displays a different output on the OmniSwitch 9900.

Examples

The following command example shows the fields that are displayed on all OmniSwitch platforms, except for the OmniSwitch 9900:

```
-> show interfaces accounting
1/1/39:
   Rx Undersize            =                  0, Tx Undersize    =           0,
   Rx Oversize             =                  0, Tx Oversize     =           0,
   Rx Jabber               =                  0,
   Rx/Tx 64 Octets         =          312890503,
   Rx/Tx 65 ~ 127 Octets   =           10496825,
   Rx/Tx 128 ~ 255 Octets  =             189426,
   Rx/Tx 256 ~ 511 Octets  =              39328,
   Rx/Tx 512 ~ 1023 Octets =                756,
   Rx/Tx 1024 ~ 1518 Octets =              48551,
   Rx/Tx 1519 ~ 4095 Octets =                  0,
   Rx/Tx 4096 ~ MAX Octets  =                  0
```

The following command example shows the fields that are displayed on an OmniSwitch 9900 (the “Rx/Tx 1024 - MAX Octets” field replaces the “Rx/Tx 1024 - 1518 Octets”, “Rx/Tx 1519 - 4095 Octets”, and “Rx/Tx 4096 - MAX Octets” fields that are displayed on the other platforms:

```
-> show interfaces accounting
1/4/38:
  Rx Undersize            =                  0, Tx Undersize    =            0,
  Rx Oversize             =                  0, Tx Oversize     =            0,
  Rx Jabber               =                  0,
  Rx/Tx 64 Octets         =          361616757,
  Rx/Tx 65 ~ 127 Octets   =           20510941,
  Rx/Tx 128 ~ 255 Octets  =             377413,
  Rx/Tx 256 ~ 511 Octets  =              45391,
  Rx/Tx 512 ~ 1023 Octets =               2319,
  Rx/Tx 1024 ~ MAX Octets =              63555,
```

output definitions

Rx Undersize	Number of undersized packets received.
Tx Undersize	Number of undersized packets transmitted.
Rx oversize	Number of oversized packets received.
Tx oversize	Number of oversized packets transmitted.
Rx Jabber	Number of Jabber packets received (longer than 1518 octets).
Rx/Tx Octets	Number of packets received and transmitted in each listed octet range.

Release History

Release 7.1.1; command introduced.
Release 8.3.1; display updated for OmniSwitch 9900.

Related Commands

interfaces ddm	Displays general interface information (e.g., hardware, MAC address, and input/output errors).
show interfaces counters	Displays interface counter information (e.g., unicast packets received/transmitted).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
dot3StatsTable
   dot3StatsFrameTooLong
   dot3StatsDeferredTransmissions
alcetherStatsTable
   alcetherStatRxsUndersizePkts
   alcetherStatTxsUndersizePkts
   alcetherStatsTxOversizePkts
   alcetherStatsPkts64Octets
   alcetherStatsPkts65to127Octets
   alcetherStatsPkts128to255Octets
   alcetherStatsPkts256to511Octets
   alcetherStatsPkts512to1023Octets
   alcetherStatsPkts1024to1518Octets
   gigaEtherStatsPkts1519to4095Octets
   gigaEtherStatsPkts4096to9215Octets
   alcetherStatsRxJabber
```

show interfaces counters

Displays interface counters information (e.g., unicast, broadcast, and multi-cast packets received/ transmitted).

show interfaces [slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***]] counters**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If no slot/port numbers are entered, counter information for all slots/ports on the switch is displayed.

Examples

```
-> show interfaces port 1/3/1 counters
1/3/1 ,
InOctets      = 54367578586897979,  OutOctets     = 5.78E19,
InUcastPkts   = 55654265276,        OutUcastPkts  = 5.78E20,
InMcastPkts   = 58767867868768777,  OutMcastPkts  = 5465758756856,
InBcastPkts   = 576567567567567576, OutBcastPkts  = 786876,
InPauseFrames = 567798768768767,    OutPauseFrames= 786876,
```

output definitions

InOctets	Number of octets received.
OutOctets	Number of octets transmitted.
InUcastPkts	Number of unicast packets received.
OutUcastPkts	Number of unicast packets transmitted.
InMcastPkts	Number of multicast packets received.
OutMcastPkts	Number of unicast packets transmitted.
InBcastPkts	Number of broadcast packets received.
OutBcastPkts	Number of unicast packets transmitted.
InPauseFrames	Number of MAC control frames received.
OutPauseFrames	Number of MAC control frames transmitted.

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces counters errors	Displays interface error frame information (e.g., CRC errors, transit errors, and receive errors).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
ifXTable
   IfHCInOctets
   IfHCOutOctets
   IfHCInUcastPkts
   IfHCOutUcastPkts
   IfHCInMulticastPkts
   IfHCOutMulticastPkts
   IfHCInBroadcastPkts
   IfHCOutBroadcastPkts
dot3PauseTable
   dot3InPauseFrame
   dot3OutPauseFrame
```

show interfaces counters errors

Displays interface error frame information (e.g., CRC errors, transit errors, and receive errors).

show interfaces [slot *chassis/slot* **| port** *chassis/slot/port***[-***port2***]] counters errors**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If no slot/port numbers are entered, counter error information for all slots/ports on the switch is displayed.

Examples

```
-> show interfaces port 1/2/1 counters errors
1/2/1 ,
  Alignments Errors = 6.45E13,  FCS Errors = 7.65E12
  IfInErrors        = 6435346,  IfOutErrors = 5543,
  Undersize pkts    = 867568, Oversize pkts = 5.98E8
```

output definitions

Chas/Slot/Port	Interface chassis, slot, and port number.
Alignments Errors	Number of Alignments errors.
FCS Errors	Number of Frame Check Sequence errors.
IfInErrors	Number of received error frames.
IfOutErrors	Number of transmitted error frames.
Undersize pkts	Number of undersized packets.
Oversize pkts	Number of oversized packets (more than 1518 octets).

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces counters	Displays interface counters information (e.g., unicast, broadcast, and multi-cast packets received/transmitted).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
ifTable
   ifInErrors
   ifOutErrors
alcetherStatsTable
   alcetherStatsRxUndersizePkts
dot3StatsTable
   dot3StatsAlignmentErrors
   dot3StatsFCSErrors
   dot3StatsFrameTooLong
```

show interfaces flood-rate

Displays interface peak flood rate settings.

show interfaces [slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***]] flood-rate**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show interfaces flood-rate
 Chas/
 Slot/  Bcast    Bcast   Bcast   Ucast    Ucast   Ucast    Mcast   Mcast   Mcast
 Port   Value     Type  Status   Value     Type  Status    Value    Type  Status
-----+----------+-----+-------+----------+-----+-------+----------+-----+--------
1/1/1        496  mbps  enable        496  mbps  enable        496  mbps disable
1/1/2        496  mbps  enable        496  mbps  enable        496  mbps disable
1/1/3        496  mbps  enable        496  mbps  enable        496  mbps disable
1/1/4        496  mbps  enable        496  mbps  enable        496  mbps disable
1/1/5        496  mbps  enable        496  mbps  enable        496  mbps disable
```

output definitions

Slot/Port	Interface slot and port numbers.
Value	The value set based on the type of flood limiting.
Type	The type of flood limiting: mbps, pps, or %
Status	Status of the type of flood-limiting: enbaled or disabled.

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces flood-limit	Configures the peak flood rate for an interface.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortMaxFloodRate
   esmPortFloodMcastEnable
```

show interfaces traffic

Displays interface traffic statistics.

show interfaces [slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***]] traffic**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If no slot/port numbers are entered, traffic settings for all slots/ports on the switch are displayed.

Examples

```
-> show interfaces traffic
 Ch/Slot/Port   Input packets     Input bytes      Output packets    Output bytes
------------+-----------------+-----------------+-----------------+--------------
 1/1/2               322             20624             5125            347216
 1/3/2               322             20620             5133            347764
```

output definitions

Ch/Slot/Port	Interface chassis, slot, and port numbers.
Input packets	Input packets detected.
Input bytes	Input bytes detected.
Output packets	Output packets detected.
Output bytes	Output bytes detected.

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces ddm	Displays general interface information (e.g., hardware, MAC address, and input/output errors).
show interfaces counters	Displays interface counter information (e.g., unicast packets received/transmitted).

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
ifXTable
   ifHCInOctets
   ifHCInUcastPkts
   ifHCInMulticastPkts
   ifHCInBroadcastPkts
   ifHCOutOctets
   ifHCOutUcastPkts
   ifHCOutMulticastPkts
   ifHCOutBroadcastPkts
```

show interfaces ingress-rate-limit

Displays the ingress-rate-limit set for each interface port.

show interfaces [slot *chassis/slot*| **port** *chassis/slot/port***[**-*port1***]] ingress-rate-limit**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[**-*port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If the slot number is not specified, then the switch back pressure feature must be enabled or disabled on an entire chassis.

Examples

```
-> show interfaces port 1/1/1-4 ingress-rate-limit
 Chas/
 Slot/ Rate Limit Burst Size Status
 Port    (Mbps)     (MB)
------+----------+----------+-------
 1/1/1       496         19  disable
 1/1/2       496         19  disable
 1/1/3       496         19  disable
 1/1/4       496         19  disable
```

output definitions

Chas/Slot/Port	Interface chassis, slot, and port numbers.
Rate Limit (Mbps)	Rate limit in Megabits.
Burst Size (MB)	Burst size in Megabytes.
Status	Status of rate limiting.

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces duplex	Configures the ingress-rate-limit.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
```

show interfaces ddm

Displays the Digital Diagnostics Monitoring (DDM) information for the specified transceivers.

show interfaces [slot *chassis/slot*| **port** *chassis/slot/port***[**-*port1***]] ddm [w-low | w-high | status | a-low | a-high | actual]**

Syntax Definitions

chassis	The chassis identifier.
slot	Display all the transceivers on the specified slot.
*port***[**-*port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.
w-low	Display the transceivers Warning Low value.
w-high	Display the transceivers Warning High value.
status	Display the administrative status of DDM.
a-low	Display the transceivers Alarm Low value.
a-high	Display the transceivers Alarm High value.
actual	The real-time values indicated by the transceiver. Values displayed in parentheses indicate the Warning or Alarm value that has been reached.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If the threshold values of the transceiver are ‘0’ then NS (Not Supported) will be displayed in the DDM output display.

Examples

```
-> show interfaces ddm w-low
Chas/
Slot/Port   Temp (C)   Voltage (V)   Tx Bias (mA)   Output (dBm)   Input (dBm)
---------+----------+------------+--------------+--------------+--------------
1/1         48            5.15         50              2.50          2.50
1/2         47            5.35         49              2.43          2.43
1/3         NA              NA         NA                NA            NA

-> show interfaces ddm a-high
Chas/
Slot/Port   Temp (C)   Voltage (V)   Tx Bias (mA)   Output (dBm)   Input (dBm)
---------+----------+------------+--------------+--------------+--------------
1/1/1       50            5.75         75              3.22          3.22
1/1/2       50            5.95         65              3.22          3.22
```

```
1/1/3       NA              NA          NA                NA             NA

-> show interfaces port 1/1/1 ddm
 Chas/
 Slot/     Thres-      Temp       Voltage      Tx Bias      Output       Input
 Port      hold         (C)         (V)          (mA)        (dBm)       (dBm)
---------+-----------+-------+-----------+------------+------------+-----------
1/1/1     Actual         50      1.95(WL)        75         4.92(AH)    3.22
          Alarm High     120     5.75           100         4.91        4.91
          Warning High   90      3.00            90         4.77        4.77
          Warning Low    10      2.00            60         0.00        0.00
          Alarm Low      -5      1.75            20        -3.01        -10

-> show interfaces ddm status
DDM Status      : enable
DDM Trap Status : disable
```

output definitions

Chas/Slot/Port	Interface chassis, slot, and port numbers.
Temp C	The transceiver temperature, in degrees centigrade.
Voltage (V)	The transceiver supply voltage, in volts.
Tx Bias (mA)	The transceiver transmit bias current, in milliamps.
Output (dBm)	The transceiver output power, in decibels.
Input (dBm)	The transceiver received optical power, in decibels.
N/A	Indicates the transceiver does support DDM.
N/S	Indicates the transceiver does not support the DDM attribute.
Actual	The real-time values indicated by the transceiver. Values displayed in parentheses indicate the Warning or Alarm value that has been reached.
Alarm High (AH)	Indicates the value at which the transceiver's functionality may be affected.
Warning High (WH)	Indicates the transceiver is approaching the High Alarm value.
Warning Low (WL)	Indicates the transceiver is approaching the Low Alarm value.
Alarm Low (AL)	Indicates the value at which the transceiver's functionality may be affected.
DDM Status	The administrative status of DDM.
DDM Trap Status	The administrative status of DDM traps.

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces ddm	Configures the DDM administrative status or trap capability.

MIB Objects

```
ddmNotifications
   ddmTemperature
   ddmTempLowWarning
   ddmTempLowAlarm
   ddmTempHiWarning
   ddmTempHiAlarm
   ddmSupplyVoltage
   ddmSupplyVoltageLowWarning
   ddmSupplyVoltageLowAlarm
   ddmSupplyVoltageHiWarning
   ddmSupplyVoltageHiAlarm
   ddmTxBiasCurrent
   ddmTxBiasCurrentLowWarning
   ddmTxBiasCurrentLowAlarm
   ddmTxBiasCurrentHiWarning
   ddmTxBiasCurrentHiAlarm
   ddmTxOutputPower
   ddmTxOutputPowerLowWarning
   ddmTxOutputPowerLowAlarm
   ddmTxOutputPowerHiWarning
   ddmTxOutputPowerHiAlarm
   ddmRxOpticalPower
   ddmRxOpticalPowerLowWarning
   ddmRxOpticalPowerLowAlarm
   ddmRxOpticalPowerHiWarning
   ddmRxOpticalPowerHiAlarm
```

show interfaces split-mode

Displays the configured and operational state of the 4X10G capable ports.

show interfaces [slot *chassis/slot* | **port** *chassis/slot/port***[**-*port1***]] split-mode**

Syntax Definitions

chassis	The chassis identifier.
slot	Display all the ports on the specified slot.
*port***[**-*port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

By default, information for all ports that support the splitter cable functionality is displayed.

Platforms Supported

OmniSwitch 6900, 9900

Usage Guidelines

The output is only displayed for those ports that support the splitter cable functionality.

Examples

```
-> show interfaces split-mode
 Ch/                                          Ch/
 Slot/                  Split-Mode            Slot
 Primary-Port     Configured   Operational     Member-Port
--------------+--------------+-------------+---------------
 1/1/1A               4X10         4X10G     1/1/1A-1/1/1D
 1/1/2A               AUTO         40G       1/1/2A-1/1/2D
 1/1/3A               40G          40G       1/1/3A-1/1/3D
 1/1/4A               AUTO         None      1/1/4A-1/1/4D
<output truncated>
```

output definitions

Ch/Slot/Port	The chassis, slot, and port.
Configured	The configured split-mode of the port. (AUTO/4X10G/4X25G/40G/ 100G)
Operational	The current operational split-mode of the port. (AUTO/4X10G/4X25G/ 40G//100G/None)

Release History

Release 7.3.4; command introduced.

Related Commands

interfaces primary-port split-mode	Configures the mode of the splitter cable capable ports.

MIB Objects

```
esmPortModeTable
   esmConfiguredMode
```

show transceivers

Displays transceiver manufacturer and status information.

show transceivers [slot *chassis/slot* **[transceiver** *transceiver_num***]]**

Syntax Definitions

chassis	The chassis identifier.
slot	Display all the ports on the specified slot.
transceiver_num	The number of the transceiver to display.

Defaults

By default, information is displayed for all transceivers.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify a chassis/slot number to display transceiver information for a specific module.
- Specify a transceiver model number to display information for a specific transceiver.

Examples

```
-> show transceivers
Chassis ID 1
Slot 1 Transceiver 53
  ALU Model Name:               QSFP-40G-C1M   ,
  ALU Model Number:             120387-90   ,
  Hardware Revision:            A ,
  Serial Number:                404820066       ,
  Manufacture Date:             Feb 17 2014,
  Laser Wave Length:            N/A,
  Admin Status:                 POWER ON,
  Operational Status:           UP

Chassis ID 2
Slot 1 Transceiver 30
  ALU Model Name:               QSFP-40G-C1M   ,
  ALU Model Number:             120387-90   ,
  Hardware Revision:            A ,
  Serial Number:                404820066       ,
  Manufacture Date:             Feb 17 2014,
  Laser Wave Length:            N/A,
  Admin Status:                 POWER ON,
  Operational Status:           UP

Slot 1 Transceiver 39
  Manufacturer Name:            PICOLIGHT       ,
  Part Number:                  PL-XPL-00-S13-00,
```

```
  Hardware Revision:                ,
  Serial Number:                P100Q1F         ,
  Manufacture Date:             Jul  2 2002,
  Laser Wave Length:            N/A,
  Admin Status:                 POWER ON,
  Operational Status:           UP

-> show transceivers slot 2/1
Slot 1 Transceiver 30
  ALU Model Name:               QSFP-40G-C1M   ,
  ALU Model Number:             120387-90   ,
  Hardware Revision:            A ,
  Serial Number:                404820066       ,
  Manufacture Date:             Feb 17 2014,
  Laser Wave Length:            N/A,
  Admin Status:                 POWER ON,
  Operational Status:           UP

Slot 1 Transceiver 39
  Manufacturer Name:            PICOLIGHT       ,
  Part Number:                  PL-XPL-00-S13-00,
  Hardware Revision:                ,
  Serial Number:                P100Q1F         ,
  Manufacture Date:             Jul  2 2002,
  Laser Wave Length:            N/A,
  Admin Status:                 POWER ON,
  Operational Status:           UP

-> show transceivers slot 2/1 transceiver 39
Slot 1 Transceiver 39
  Manufacturer Name:            PICOLIGHT       ,
  Part Number:                  PL-XPL-00-S13-00,
  Hardware Revision:                ,
  Serial Number:                P100Q1F         ,
  Manufacture Date:             Jul  2 2002,
  Laser Wave Length:            N/A,
  Admin Status:                 POWER ON,
  Operational Status:           UP
```

output definitions

Manufacturer Name	The name of the transceiver's manufacturer.
Part Number	The part number of the transceiver.
Hardware Revision	The hardware revision of the transceiver.
Serial Number	The serial number of the transceiver.
Manufacture Date	The manufacture date of the transceiver.
Laser Wave Length	The laser wavelength of the transceiver.
Admin Status	The administrative status of the transceiver.
Operational Status	The operational status of the transceiver.

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces ddm	Displays the DDM administrative status or trap capability.

MIB Objects

N/A

show violation

Displays the violation conditions that exist on specific ports or link aggregates.

show violation [port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]]**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.
*agg_id***[-***agg_id2***]**	Enter a link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

NA

Examples

In the following example, the **admin down** action for link aggregate 2 indicates that a port violation has occurred on one of the ports related to the link aggregate group with ID 2.

```
-> show violation
* = Link Agg ID
 LAG ID/                                                    Recovery     Recovery
 Port       Source         Action            Reason      WTR   Time      Max/Remain
----------+----------+-----------------+--------------+-----+---------+----------
  1/1/1    src lrn    simulated down      lps shutdown     0      300      10/5
  1/1/1    src lrn    simulated down      lps restrict     0      300      10/10
 *0/2      qos        admin down          policy           0      300      10/10
```

output definitions

Port	The slot and port numbers or link aggregate IDs on which violations occurred.
Source	Specifies the source application that detected the violation.
Action	Specifies the action that is taken when the violation is detected on the port. There are two types of actions: **admin down** - deactivates the physical port. **simulated down** - the port is put in blocking state.
Reason	Specifies the reason for the violation.

output definitions\

WTR	The wait-to-restore timer value. Specifies the number of seconds the switch waits before notifying other applications that the link is up. Configured through the **interfaces wait-to-restore** command.
Recovery Time	The amount of time after which the port is automatically re-activated if the port was shutdown. Configured through the **violation recovery-time** command.
Recovery Max/Remain	The maximum number of recovery attempts allowed and the number of attempts remaining. Configured through the **violation recovery-maximum** command.

Release History

Release 7.1.1; command introduced.

Related Commands

clear violation	Clears all the MAC address violation logs for a particular port and session. After the violations are cleared, the specific port resumes normal operation.

MIB Objects

```
portViolationTable
   portViolationSource
   portViolationEntry
   portViolationTrap
   portViolationSource
   portViolationReason
   portViolationAction
   portViolationTimer
   portViolationTimerAction
```

show violation-recovery-configuration

Displays the global violation recovery configuration details (recovery trap, recovery maximum, and recovery time.

show violation-recovery-configuration {slot *chassis/slot* **| port** *chassis/slot/port***[-***port2***]}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

NA

Examples

```
-> show violation-recovery-configuration
Global Violation Trap         : enable
Global Recovery Maximum       : 20
Global Recovery Time          : 200

Port    Recovery Max    Recovery Time
------+---------------+---------------
1/1/1   10                    300
1/1/2   10                    300

-> show violation-recovery-configuration port 3/1/1-2
Global Recovery Trap          : enable
Global Recovery Maximum       : 20
Global Recovery Time          : 200

Port   Recovery Max      Recovery Time
------+---------------+---------------
3/1/1   10                    300
3/1/2   10                    300
```

output definitions\

Global Violation Trap	Displays the global status of the violation trap recovery.
Global Recovery Maximum	Displays the global value set for the maximum violation recovery.
Global Recovery Time	Displays the global value set for the recovery time.

output definitions\

Port	Displays the chassis, slot and port numbers or link aggregate IDs on which address violations occurred.
Recovery Max	Displays the maximum number of retry configured.
Recovery Time	Displays the duration taken for recovery.

Release History

Release 8.2.1; command introduced.

Related Commands

clear violation	Clears all the MAC address violation logs for a particular port and session. After the violations are cleared, the specific port resumes normal operation.
violation recovery-maximum	Configures the maximum number of recovery attempts allowed before the port is permanently shut down.
violation recovery-time	Configures the time interval after which the port is automatically re-activated if the port was shutdown for any violation.
violation recovery-trap	Enables or disables the sending of a violation recovery trap when any port is re-enabled after the violation recovery time has expired.

MIB Objects

```
portViolationTable
   alaPvrGlobalTrapEnable
   alaPvrGlobalRetryTime
   alaPvrGlobalRecoveryMax
   alaPvrRetryTime
   alaPvrRecoveryMax
```

interfaces link-monitoring admin-status

Enables or disables link monitoring on a specific slot, port, or a range of specified ports.

interfaces {slot *chassis/slot* | **port** *chassis/slot/port***[**-*port2***]} link-monitoring admin-status {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
enable	Enables link monitoring for the specified port.
disable	Disables link monitoring for the specified port.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Configuring link monitoring parameters are allowed even if the link monitoring status is disabled for the specified ports.
- The Automatic Recovery Timer and link monitoring must not be enabled on Remote Fault Propagation (RFP) enabled ports.
- Enter a slot number to configure link monitoring for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure link monitoring for a specific interface or range of interfaces.
- Link Monitoring can be enabled on the member ports of the link aggregate, but not on the entire link aggregate. Link Monitoring is not supported on the VFL ports.

Example

```
-> interfaces slot 1/1 link-monitoring admin-status enable
-> interfaces port 1/1/1 link-monitoring admin-status enable
-> interfaces port 1/1/1-7 link-monitoring admin-status enable
-> interfaces port 1/2/5 link-monitoring admin-status disable
-> interfaces port 1/2/5-20 link-monitoring admin-status disable
```

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces ddm	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonStatus
```

interfaces link-monitoring time-window

Configures the monitoring time window on a specific slot, port, or a range of specified ports. This is the length of time during which the link is monitored.

interfaces {slot *chassis/slot* | **port** *chassis/slot/port***[**-*port2***]} link-monitoring time-window** *seconds*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
seconds	The length of time during which the link is monitored. The valid range is 0–3600 seconds.

Defaults

By default, the time window value is set to 300 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a slot number to configure the monitoring time window for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the monitoring time window for a specific interface or a range of interfaces.

Example

```
-> interfaces slot 1/1 link-monitoring time-window 20
-> interfaces port 1/1/1 link-monitoring time-window 40
-> interfaces port 1/1/1-7 link-monitoring time-window 2500
```

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces link-monitoring config	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonTimeWindow
```

interfaces link-monitoring link-flap-threshold

Configures the number of link flaps allowed on a specific slot, port, or a range of specified ports in the time interval, before the port is shutdown.

interfaces {slot *chassis/slot* | **port** *chassis/slot/port***[**-*port2***]} link-monitoring link-flap-threshold** *link_flaps*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.
link_flaps	The number of link flaps. The valid range is 2-10.

Defaults

By default, the number of link flaps allowed is set to 5.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a slot number to configure the number of link flaps allowed for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the number of link flaps allowed for a specific interface or a range of interfaces.

Example

```
-> interfaces slot 1/1 link-monitoring link-flap-threshold 6
-> interfaces port 1/1/1 link-monitoring link-flap-threshold 3
-> interfaces port 1/1/1-7 link-monitoring link-flap-threshold 10
```

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces ddm	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonLinkFlapThreshold
```

interfaces link-monitoring link-error-threshold

Configures the number of MAC errors allowed on a specific slot, port, or a range of specified ports in the time interval, before the port is shutdown. MAC errors refer to lost frames, error frames, alignment frames and cyclic redundancy check (CRC).

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} link-monitoring link-error-threshold** *mac_errors*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.
mac_errors	The number of MAC errors. The valid range is 1-100.

Defaults

By default, the number of MAC errors allowed is set to 5.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a slot number to configure the number of MAC errors allowed on all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the number of MAC errors allowed on a specific interface or on a range of interfaces.

Example

```
-> interfaces slot 1/1 link-monitoring link-error-threshold 30
-> interfaces port 1/1/1 link-monitoring link-error-threshold 10
-> interfaces port 1/1/1-7 link-monitoring link-error-threshold 35
```

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces ddm	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonLinkErrorThreshold
```

interfaces clear-link-monitoring-stats

Clears the link monitoring statistics on a specific slot, port, or a range of specified ports.

interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[**-*port2***]} clear-link-monitoring-stats**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a slot number to clear monitoring statistics for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to clear monitoring statistics for a specific interface or a range of interfaces.

Example

```
-> interfaces slot 1/1 clear-link-monitoring-stats
-> interfaces port 1/1/1 clear-link-monitoring-stats
-> interfaces port 1/1/1-7 clear-link-monitoring-stats
```

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces ddm	Displays the link monitoring configuration for the specified ports.
show interfaces link-monitoring statistics	Displays the link monitoring statistics for the specified ports.

MIB Objects

```
alaLinkMonStatsTable
   alaLinkMonStatsClearStats
```

show interfaces link-monitoring config

Displays configuration information for the Link Monitoring feature. This includes the link monitoring status on a specific slot, port or a range of specified ports, time window, link flap threshold, and link error threshold.

show interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[-***port2***]} link-monitoring config**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific port.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Example

```
-> show interfaces slot 1/1 link-monitoring config
Ch/
Slot/   Status   Time     Link-flap    Link-error
Port             Window   Threshold    Threshold
                 (sec)
------+--------+--------+------------+-----------
1/1/1  enabled     10        5           10
1/1/2  disabled    10        5           10
1/1/3  disabled   200        8           20
.
.
1/1/24 disabled   150        2           99

-> show interfaces port 1/1/1-3 link-monitoring config
Ch/
Slot/   Status   Time      Link-flap    Link-error
Port             Window    Threshold    Threshold
                 (sec)
------+--------+--------+------------+-------------
1/1/1  enabled     10         5            10
1/1/2  disabled    10         5            10
1/1/3  disabled   200         7            99
```

```
-> show interfaces port 1/1/1 link-monitoring config
Ch/
Slot/   Status    Time     Link-flap    Link-error
Port              Window   Threshold    Threshold
                  (sec)
------+--------+--------+------------+-------------
1/1/1  enabled     10          5           10

-> show interfaces port 1/1/2 link-monitoring config
Ch/
Slot/   Status    Time     Link-flap    Link-error
Port              Window   Threshold    Threshold
                  (sec)
------+--------+--------+------------+------------
1/1/2  disabled    10         5            10
```

output definitions

Ch/Slot/Port	Interface chassis, slot, and port number.
Status	Link monitoring status (enable/disable).
Time Window	Time interval, in seconds, for which the link is monitored.
Link-flap threshold	Number of link flaps allowed on a specific slot, port, or a range of specified ports in the time interval before the port is shutdown.
Link-error threshold	Number of MAC errors allowed on a specific slot, port, or a range of specified ports in the time interval before the port is shutdown.

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays information of the interface port status.
show interfaces link-monitoring statistics	Displays the Link Monitoring statistics.
interfaces link-monitoring admin-status	Enables or disables link monitoring.
interfaces link-monitoring time-window	Configures the monitoring of the time-window of the link.
interfaces link-monitoring link-flap-threshold	Configures the number of link flaps that are allowed before the port is shutdown.
interfaces link-monitoring link-error-threshold	Configures the number of MAC errors that are allowed before the port is shutdown.

MIB Objects

```
alaLinkMonConfigTable
   alaLinkMonStatus
   alaLinkMonTimeWindow
   alaLinkMonLinkFlapThreshold
   alaLinkMonLinkErrorThreshold
```

show interfaces link-monitoring statistics

Displays the Link Monitoring statistics for a specific slot, port, or a range of specified ports.

show interfaces {slot *chassis/slot*| **port** *chassis/slot/port***[-***port2***]} link-monitoring statistics**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific port.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

Example

```
-> show interfaces slot 1/1 link-monitoring statistics
Ch/
Slot/   State     Current  Current  Current   Current  Current  Total  Total
Port              Flap     Error    CRC       Lost     Align    Flap   Error
------+---------+--------+--------+--------+--------+--------+-------+-------+
1/1/1   shutdown    6       3         2         0         0       15      6
1/1/2   down        3       2         1         0         0       12      3
.
.
1/1/24   up         3       2         1          0        0       12      3

-> show interfaces port 1/1/1-2 link-monitoring statistics
Ch/
Slot/   State     Current  Current  Current   Current  Current  Total  Total
Port              Flap     Error    CRC       Lost     Align    Flap   Error
------+---------+--------+--------+--------+--------+--------+-------+-------+
1/1/1   shutdown    6       3         2         0         0       15      6
1/1/2   down        3       2         1         0         0       12      3

-> show interfaces port 1/1/1 link-monitoring statistics
Ch/
Slot/   State     Current  Current  Current   Current  Current  Total  Total
Port              Flap     Error    CRC       Lost     Align    Flap   Error
------+---------+--------+--------+--------+--------+--------+-------+-------+
1/1/1   shutdown    6       3         2         0         0       15      6
```

Release History

Release 7.3.2; command introduced.

Related Commands

show interfaces	Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
show interfaces link-monitoring config	Displays configuration information of the Link Monitoring.
interfaces link-monitoring admin-status	Enables or disables link monitoring.
interfaces clear-link-monitoring-stats	Clears the Link Monitoring statistics.
interfaces link-monitoring link-error-threshold	Configures the number of MAC errors that are allowed before the port is shutdown.

MIB Objects

```
alaLinkMonStatsTable
   alaLinkMonStatsPortStatus
   alaLinkMonStatsCurrentLinkFlaps
   alaLinkMonStatsCurrentErrorFrames
   alaLinkMonStatsCurrentCRCErrors
   alaLinkMonStatsCurrentLostFrames
   alaLinkMonStatsCurrentAlignErrors
   alaLinkMonStatsCurrentLinkErrors
   alaLinkMonStatsTotalLinkFlaps
   alaLinkMonStatsTotalLinkErrors
```

interfaces tdr

Initiates a Time Domain Reflectometry (TDR) cable diagnostics test on the specified port. The TDR feature sends a signal down a cable to determine the distance to a break or other discontinuity in the cable path. The length of time it takes for the signal to reach the break and return is used to estimate the distance to the discontinuity.

interfaces port *chassis/slot/port* **tdr enable**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
port	The port number.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- TDR is an on-demand, out-of-service test. The test is not automatically triggered; data and protocol traffic is interrupted.
- Only one TDR test can be run at any given time.
- TDR is not supported on link aggregate ports, fiber ports, or stacking ports.
- TDR results are automatically cleared when a new test is started on the port or when the module for the port is reset.

Examples

```
-> interfaces port 1/1/1 tdr enable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

clear interfaces	Clears the statistics of the last test performed on the port
show interfaces tdr-statistics	Displays the results of the last TDR test performed on a port.

MIB Objects

```
esmTdrPortTable
   esmTdrPortTest
```

show interfaces tdr-statistics

Displays the results of the last TDR test performed on a port.

show interfaces [slot *chassis/slot* | **port** *chassis/slot/port***[-***port2***]] tdr-statistics**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[-***port2***]**	The port number. Use a hyphen to specify a range of ports.

Defaults

By default, TDR statistics are shown for all ports on all modules

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or range of interfaces.

Examples

```
-> show interfaces port 1/1/3 tdr-statistics
 Ch/
 Slot/  No of Fuzzy Pair1 Pair1 Pair2 Pair2 Pair3 Pair3 Pair4 Pair4  Test
 Port   Pairs Len   State Len   State Len   State Len   State Len   Results
-------+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+--------
1/1/1     4   10    Open  0     Open  0     Open  0     Open  0     Success

Pair Length Accuracy may vary +/- Fuzzy Length
Legend: Pair 1 - Orange and White
        Pair 2 - Green and White
        Pair 3 - Blue and White
        Pair 4 - Brown and White
```

output definitions

Ch/Slot/Port	The interface chassis, slot, and port number.
No of pairs	The number of pairs in the cable for which the test results are valid.
Fuzzy Length	The error in the estimated length of the cable.

output definitions (continued)

Cable State	State of a cable as returned by the TDR test. The state of the cable wire. (a) **OK** - Wire is working properly (b) **Open** - Wire is broken (c) S**hort** - Pairs of wire are in contact with each other (d) **Crosstalk** - Signal transmitted on one pair of wire creates an undesired effect in another wire. (e) **Unknown** - Cable diagnostic test unable to find the state of a cable.
Pair1 State	The state of the Pair 1 cable wire (**OK**, **Open**, **Short**, **Crosstalk**, or **Unknown**)
Pair1 Length	The length of the Pair 1 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.
Pair2 State	The state of the Pair 2 cable wire (**OK**, **Open**, **Short**, **Crosstalk**, or **Unknown**)
Pair2 Length	The length of the Pair 2 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.
Pair3 State	The state of the Pair 3 cable wire (**OK**, **Open**, **Short**, **Crosstalk**, or **Unknown**)
Pair3 Length	The length of the Pair 3 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.
Pair4 State	The state of the Pair 4 cable wire (**OK**, **Open**, **Short**, **Crosstalk**, or **Unknown**)
Pair4 Length	The length of the Pair 4 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.
Test Result	The status of the TDR test performed, success or fail.
Legend	Eight-conductor data cable contains 4 pairs of twisted Pair Copper Cable wires. Each pair consists of a solid (or predominantly) colored wire and a white wire with a strip of the same color. The pairs are twisted together.

Release History

Release 8.1.1 command was introduced.

Related Commands

interfaces tdr	Initiates the cable diagnostics on a port.
clear interfaces	Clears the statistics of the last test performed on the port.

MIB Objects

```
esmTdrPortTable
   esmTdrPortCableState
   esmTdrPortValidPairs
   esmTdrPortPair1State
   esmTdrPortPair1Length
   esmTdrPortPair2State
   esmTdrPortPair2Length
   esmTdrPortPair3State
   esmTdrPortPair3Length
   esmTdrPortPair4State
   esmTdrPortPair4Length
   esmTdrPortFuzzLength
```

link-fault-propagation group

Configures a Link Fault Propagation (LFP) group to associate with source and destination ports.

link-fault-propagation group *group_id* **[admin-status {enable | disable}]**

no link-fault-propagation group {*group_id***[-***group_id2***]}**

Syntax Definitions

group_id	A group ID number. The valid range is 1–8.
*group_id***[-***group_id2***]**	A group ID number to remove. Use a hyphen to specify a range of existing group ID numbers (5-8). Specifying a range is only used to remove group IDs, not to create them.
enable	Enables LFP for the specified group.
disable	Disables LFP for the specified group.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a LFP group or a range of groups.
- Up to eight LFP groups per switch are allowed.
- Once a LFP group is created, assign source and destination ports to that group.

Example

```
-> link-fault-propagation group 1
-> no link-fault-propagation group 4
-> no link-fault-propagation group 4-7
```

Release History

Release 7.3.2; command introduced.

Related Commands

link-fault-propagation group source	Configures the source port assignments for the LFP group.
link-fault-propagation group destination	Configures the destination port assignments for the LFP group.
link-fault-propagation group wait-to-shutdown	Configures the amount of time LFP waits before shutting down the destination ports.
show link-fault-propagation group	Displays the LFP group configuration for the switch.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
   alaLFPGroupRowStatus
```

link-fault-propagation group source

Configures the source port assignments for a Link Fault Propagation (LFP) group.

link-fault-propagation group *group_id* **source {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

no link-fault-propagation group *group_id* **source {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

Syntax Definitions

group_id	An existing LFP group ID number. The valid range is 1–8.
chassis	The chassis identifier.
slot	The slot number for a specific module.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports and/or a space to specify multiple port entries.
agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs and/or a space to specify multiple ID entries (1-5 10 12).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a source port association with the specified LFP group.
- Make sure the LFP group specified with this command already exists in the switch configuration.
- Configuring the source ports and destinations ports for the specified LFP group is allowed within the same command (see the examples on this command page).
- A group can have a maximum of 64 source ports and 64 destination ports.
- A maximum of 64 link aggregates is supported, regardless of the number of ports in each aggregate in a group.
- A port/linkagg added as a source/destination port for a particular group cannot be added as a destination/source port for this group or for any other group.
- If a port is recovered due to the Interface Recovery Timer, then the port will revert to the shutdown state if the error persists.

Example

```
-> link-fault-propagation group 1 source port 1/2
-> link-fault-propagation group 1 source port 1/2-5 2/3
-> link-fault-propagation group 1 source linkagg 1
```

```
-> link-fault-propagation group 1 source linkagg 1-3
-> link-fault-propagation group 1 source port 2/3 destination port 1/6
-> link-fault-propagation group 1 source port 3/1-5 destination linkagg 6
-> no link-fault-propagation group 1 destination port 1/10
```

Release History

Release 7.3.2; command introduced.

Related Commands

link-fault-propagation group	Configures an LFP group, including the administrative status.
link-fault-propagation group destination	Configures the destination port assignments for the LFP group.
link-fault-propagation group wait-to-shutdown	Configures the amount of time LFP waits before shutting down the destination ports.
show link-fault-propagation group	Displays the LFP group configuration for the switch.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
alaLFPConfigTable
   alaLFPConfigPort
   alaLFPConfigPortType
   alaLFPConfigRowStatus
```

link-fault-propagation group destination

Configures the destination port assignments for a Link Fault Propagation (LFP) group.

link-fault-propagation group *group_id* **destination {port** *chassis/slot/port[-port2]* **| linkagg** *agg_id[-agg_id2]***}**

no link-fault-propagation group *group_id* **destination {port** *chassis/slot/port[-port2]* **| linkagg** *agg_id[-agg_id2]***}**

Syntax Definitions

group_id	An existing LFP group ID number. The valid range is 1–8.
chassis	The chassis identifier.
*port***[**-*port2***]**	The port number. Use a hyphen to specify a range of ports and/or a space to specify multiple port entries.
agg_i*d***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs and/or a space to specify multiple ID entries (1-5 10 12).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a destination port association with the specified LFP group.
- Make sure the LFP group specified with this command already exists in the switch configuration.
- Configuring the source ports and destinations ports for the specified LFP group is allowed within the same command (see the examples on this command page).
- A group can have a maximum of 64 source ports and 64 destination ports.
- A maximum of 64 link aggregates is supported regardless of the number of ports in each aggregate in a group.
- A port or link aggregate that is configured as a source port cannot be configured as a destination port for any group. However, a source port can be associated with multiple LFP groups.
- A port or link aggregate that is configured as a destination port cannot be configured as a source port for any group. However, a destination port can be associated with multiple LFP groups.
- If port is recovered due to the Interface Recovery Timer, then the port will revert to the shutdown state if the error persists.

Example

```
-> link-fault-propagation group 1 destination port 1/4
-> link-fault-propagation group 1 destination port 1/5-8 2/3
-> link-fault-propagation group 1 destination linkagg 6
-> link-fault-propagation group 1 destination linkagg 6-10
-> link-fault-propagation group 1 source port 1/2 2/3 destination port 1/6
-> link-fault-propagation group 1 source port 1/2 2/3 destination linkagg 6
-> link-fault-propagation group 1 source linkagg 3 destination port 1/6 1/9
-> link-fault-propagation group 1 source linkagg 3 destination linkagg 1

-> no link-fault-propagation group 1 source port 1/9
-> no link-fault-propagation group 1 destination port 1/10
```

Release History

Release 7.3.2; command introduced.

Related Commands

link-fault-propagation group	Configures an LFP group, including the administrative status.
link-fault-propagation group source	Configures the source port assignments for the LFP group.
link-fault-propagation group wait-to-shutdown	Configures the amount of time LFP waits before shutting down the destination ports.
show link-fault-propagation group	Displays the LFP group configuration for the switch.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
alaLFPConfigTable
   alaLFPConfigPort
   alaLFPConfigPortType
   alaLFPConfigRowStatus
```

link-fault-propagation group wait-to-shutdown

Configures the wait-to-shutdown timer value for the Link Fault Propagation (LFP) group. This is the amount of time after all the source ports go down that LFP waits before shutting down the destination ports.

link-fault-propagation group *group_id* **wait-to-shutdown** *seconds*

Syntax Definitions

group_id	An existing LFP group ID number. The valid range is 1–8.
seconds	The number of seconds LFP waits before shutting down the destination ports. The valid range is 0-300 in multiples of 5.

Defaults

By default, the timer is set to zero (disabled).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Set the wait-to-shutdown timer value to 0 to disable the timer.
- Make sure the LFP group specified with this command already exists in the switch configuration.

Example

```
-> link-fault-propagation group 1 wait-to-shutdown 40
-> link-fault-propagation group 3 wait-to-shutdown 70
-> link-fault-propagation group 5 wait-to-shutdown 0
```

Release History

Release 7.3.2; command introduced.

Related Commands

link-fault-propagation group	Configures an LFP group, including the administrative status.
show link-fault-propagation group	Displays the LFP group configuration for the switch.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
   alaLFPGroupWaitToShutdown
   alaLFPGroupRowStatus
```

show link-fault-propagation group

Displays information for the specified Link Fault Propagation (LFP) group.

show link-fault-propagation group [*group_id***]**

Syntax Definitions

group_id	An existing LFP group ID number. The valid range is 1–8.

Defaults

By default, information is displayed for all existing LFP groups.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a LFP group ID number with this command to display information for a specific group.
- If a virtual port such as a link aggregate is configured as a source or destination port it will be displayed instead of the physical ports.

Example

```
-> show link-fault-propagation group
Group Id : 2
  Source Port(s)          : 0/1-2 1/1/1-5 1/1/7,
  Destination Port(s)     : 0/3 1/1/10-13,
  Group-Src-Ports Status  : up,
  Admin Status            : enable,
  Wait To Shutdown        : 10

Group Id : 7
  Source Port(s)          : 1/1/1 1/1/3,
  Destination Port(s)     : 0/3 1/1/5 1/1/7 1/1/11 1/1/13 1/1/15 1/1/17 1/1/19 1/1/
21 1/1/23,
  Group-Src-Ports Status  : up,
  Admin Status            : enable,
  Wait To Shutdown        : 100

-> show link-fault-propagation group 2
Group Id : 2
  Source Port(s)          : 0/1-2 1/1/1-5 1/1/7,
  Destination Port(s)     : 0/3 1/1/10-13,
  Group-Src-Ports Status  : up,
  Admin Status            : enable,
  Wait To Shutdown        : 10
```

Release History

Release 7.3.2; command introduced.

Related Commands

link-fault-propagation group	Configures a LFP group, including the administrative status.
link-fault-propagation group wait-to-shutdown	Configures the amount of time LFP waits before shutting down the destination ports.

MIB Objects

```
alaLFPConfigTable
   alaLFPConfigPort
   alaLFPConfigPortType
alaLFPGroupTable
   alaLFPGroupId
      alaLFPGroupAdminStatus
      alaLFPGroupOperStatus
      alaLFPGroupWaitToShutdown
```

interfaces beacon

Configures the LED color and behavior for a port or group of ports.

interfaces {slot *chassis/slot* **| port** *chassis/slot/port[-port2]***} beacon [admin-status {enable | disable}] [led-color** *color***] [led-mode {solid | activity}]**

no interfaces {slot *chassis/slot* **| port** *chassis/slot/port[-port2]***} beacon**

Syntax Definitions

chassis	The chassis ID for the switch on which the LEDs are being configured. For standalone switches, use **1**.
slot	The slot ID for the switch on which the LEDs are being configured. For standalone switches, use **1**.
port	The port number of the interface LED you want to configure.
-port2	The last port number in a range of interface LEDs you want to configure. Be sure to insert a hyphen between port range numbers (for example, **7-10**)
led-mode	Indicates that LED behavior (activity or solid) is being configured for the corresponding interface LEDs.
activity	The LEDs will blink when traffic is detected on the corresponding ports.
solid	The LEDs will remain solid whether or not traffic is detected on the corresponding ports.
led-color	Indicates that the LED color is being configured for the corresponding port(s).
color	The color to be displayed on the corresponding port LED(s). Options include **yellow**, **white**, **red**, **magenta**, **green**, **blue**, **aqua** and **off**.
admin-status	Indicates that the beacon LED administrative status is being configured for the corresponding port(s).
enable	Enables the beacon function on the corresponding port(s).
disable	Disables the beacon function on the corresponding port(s).
no	Adding the no syntax to the beginning of the command clears all information stored in the beacon settings table. Refer to Usage Guidelines below for more information.

Defaults

parameter	default
led-mode	activity
led-color	magenta
admin-status	enable

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- Supported on the OmniSwitch 6900-Q32 and X72 models only.
- The **no interfaces beacon** command syntax clears the beacon settings from the **show interfaces beacon** table and resets LEDs to original factory-set behavior. (Once stored beacon settings are cleared, they can no longer be retrieved and beacon settings must be reconfigured.)
- The **interfaces beacon** command is supported on all Ethernet ports on the switch. However, when specifying a range in the command line, please note that The Beacon LED feature is not supported on sub-ports 'b', 'c', or 'd' when an interface is operating in 4X10G mode. Additionally, only Solid mode is supported on sub-port 'a' for 4X10G interfaces.

Examples

```
-> interfaces port 1/1/7-10 beacon led-mode solid admin-status enable led-color
aqua
-> interfaces slot 1/1 beacon led-color magenta
-> no interfaces slot 1/1/1 beacon
```

Release History

Release 7.3.4; command introduced.

Related Commands

show interfaces beacon	Displays current interface beacon settings.

MIB Objects

```
esmPortBeaconTable
   esmPortBeaconEntry
   esmBeaconAdminState
   esmBeaconLedColor
   esmBeaconLedMode
   esmBeaconRowStatus
```

show interfaces beacon

Displays current interface beacon settings.

show interfaces [slot *chassis/slot* **| port** *chassis/slot/port***[**-*port2***]] beacon**

Syntax Definitions

chassis	The chassis ID for the switch on which beacon settings are being shown. For standalone switches, use **1**.
slot	The slot ID for the switch on which beacon settings are being shown. For standalone switches, use **1**.
port	The port number for which beacon settings are being shown.
-port2	The last port number in a range for which beacon settings are being shown. Be sure to insert a hyphen between port range numbers (for example, **7-10**)

Defaults

N/A

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

Supported on the OmniSwitch 6900-Q32 and X72 models only.

Examples

```
-> show interfaces beacon
 Ch/Slot/Port   Admin-Stat   LED-Color    LED-Mode
------------+-------------+--------------+------------
 1/1/1A          Disable     Magenta      Solid
 1/1/2A          Disable     Blue         Activity
 1/1/30A         Enable      Magenta      Solid
 1/1/31A         Enable      Off          Solid
```

output definitions

Ch/Slot/Port	The chassis/slot/port ID for the switch on which beacon settings are being shown.
Admin-Stat	The beacon administrative status (Enable/Disable).
LED-Color	The LED color being displayed on the corresponding interface LED. Options include **yellow**, **white**, **red**, **magenta**, **green**, **blue**, **aqua** and **off**.
LED-Mode	The current LED behavior on the corresponding interface LED. Options include **solid** or **activity** (default).

Release History

Release 7.3.4; command introduced.

Related Commands

interfaces beacon	Allows network administrators to change LED color and behavior from a remote location.

MIB Objects

```
esmPortBeaconTable
   esmPortBeaconEntry
   esmBeaconAdminState
   esmBeaconLedColor
   esmBeaconLedMode
   esmBeaconRowStatus
```

interfaces ptp admin-state

Enables or disables IEEE 1588 Precision Time Protocol (PTP) on all the interfaces

interfaces ptp admin-state {enable | disable} [loopback-portlist <*chassis/slot/port*> <*chassis/slot/port*>**] [***chassis/slot/port***] [priority {***num* **| default}]**

Syntax Definitions

enable	Enables the PTP end-to-end transparent clock on all the interfaces.
disable	Disables the PTP end-to-end transparent clock on all the interfaces.
chassis	The chassis identifier.
slot/port	The slot and port number (for example, 3/1).
num	Set the internal priority for the incoming PTP packet. Valid range is 1–7.
default	Sets the internal priority to the default value 5.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6860, 6865, OmniSwitch 6900-Q32, OmniSwitch 6900-X72

Usage Guidelines

- This command enables PTP end-to-end transparent clock across all ports.
- PTP end-to-end transparent clock is supported in a standalone mode (virtual chassis of one) and virtual chassis of two. PTP end-to-end on a virtual chassis of two is supported only on OmniSwitch 6900-X72.
- Single loopback port per chassis is required to support PTP in a virtual chassis of two.
- Loopback ports dedicated for PTP must not be used by any other feature. Ensure PTP is configured on unused ports.
- PTP on a virtual chassis of two is not supported on chassis ID 1.
- IGMP snooping must not be configured on PTP reserved IPv4 and IPv6 multicast addresses.
- The two 10G ports, 1/1/27 and 1/1/28 on OmniSwitch 6465-P28 does not support PTP.

Examples

```
-> interfaces ptp admin-state enable
-> interfaces ptp admin-state disable
-> interfaces ptp admin-state enable priority 4
-> interfaces ptp admin-state enable priority default
-> interfaces ptp admin-state enable loopback-portlist 2/1/12 3/1/23
WARNING: User ports 2/1/12 and 3/1/23 will be out of service for users.
```

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; OmniSwitch 6860, 6865 support for PTP added.
Release 8.5R1; OmniSwitch 6465 support for PTP added.
Release 8.5R2; **loopback-portlist** keyword added.

Related Commands

show interfaces ptp config	Displays the current IEEE 1588 Precision Time Protocol (PTP) status on the switch.

MIB Objects

```
alaPtpConfiguration
alaPtpConfigAdminStatus
alaPtpConfigPriority
alaPtpConfigMode
alaPtpLoopBackPort1
alaPtpLoopBackPort2
alaPtpLoopBackPort3
alaPtpLoopBackPort4
alaPtpLoopBackPort5
alaPtpLoopBackPort6
alaPtpLoopBackPort7
alaPtpLoopBackPort8
```

interfaces port ptp p2p

Enables or disables IEEE 1588 PTP peer-to-peer transparent clock on an interface.

interfaces port *chassis/slot/port* **ptp p2p admin-state {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (for example, 3/1).
enable	Enables the PTP peer-to-peer transparent clock on an interface.
disable	Disables the PTP peer-to-peer transparent clock on an interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- PTP must be enabled globally for PTP peer-to-peer support.
- PTP peer-to-peer supports only one-step mode.
- When peer-to-peer is enabled on a port, link delay will be computed dynamically for the corresponding link.
- Ensure Loopback0 IP interface is configured on the switch as loopback0 interface address will be used as the source IP for peer delay measurement packets. If loopback0 IP interface is not configured, then peer delay measurement feature will not work.

Examples

```
-> interfaces port 1/1/1 ptp p2p admin-state enable
-> interfaces port 1/1/1 ptp p2p admin-state disable
```

Release History

Release 8.6R1; command introduced.

Related Commands

interfaces ptp admin-state	Enables or disables IEEE 1588 Precision Time Protocol (PTP) end-to-end transparent clock on the switch.
show interfaces ptp config	Displays the current IEEE 1588 Precision Time Protocol (PTP) status on the switch.

MIB Objects

```
alaPtpPortAdminStatus
AlaIpServiceSourceIpAppIndex
```

show interfaces ptp config

Displays the current PTP status on the switch.

show interfaces ptp config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, OmniSwitch 6900-Q32, OmniSwitch 6900-X72

Usage Guidelines

N/A

Examples

```
-> show interfaces ptp config

End-to-End TC:
------------------
Admin-state                    : Enabled
Priority                       : 5
Chassis-connected              : 2
LoopBack-PortList              : 2/1/12, 3/1/23

Peer-to-Peer TC:
-----------------------
Pkt source-ip      : 1.1.1.1
Port       Admin State
--------+--------------
1/1/5      Enabled
```

output definitions

End-to-End TC:	
Admin State	The PTP end-to-end administrative status on the switch (Enable/ Disable).
Priority	The internal priority configured for the incoming PTP packet.
Chassis-connected	Number of chassis connected in a virtual chassis.
LoopBack-PortList	Configured loopback ports to support PTP end-to-end on a virtual chassis of two.
Peer-to-Peer TC:	
Pkt source-ip	Loopback0 IP interface used as the source IP for peer delay measurement packets.

output definitions (continued)

Port	The chassis, slot, and port number.
Admin State	The PTP peer-to-peer administrative status on the switch (Enable/ Disable).

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; OmniSwitch 6860, 6865 support for PTP added.
Release 8.5R1; OmniSwitch 6465 support for PTP added.
Release 8.5R2; End-to-End and Peer-to-Peer transparent clock fields added.

Related Commands

interfaces ptp admin-state	Enables or disables IEEE 1588 Precision Time Protocol (PTP) end-to-end transparent clock on the switch.
interfaces port ptp p2p	Enables or disables IEEE 1588 PTP peer-to-peer transparent clock on an interface.

MIB Objects

N/A

interfaces macsec admin-state

This command enables or disables MACsec on a physical port or a port range.

interfaces {slot *chassis/slot*| **port** *chassis/slot/port* **[**-*port2***]} macsec admin-state {enable | disable} [mode {static sci-rx [***hex-num***] key-chain** *keychain_id* **[encryption] sci-tx [***hex-num]* **key-chain** *keychain_id* **[encryption] | dynamic {keychain** *cak_keychain_id* **[server-priority** *priority***] | radius}} [transmit-interval** *tx_interval***] [encryption]]**

no interfaces {slot *chassis/slot*| **port** *chassis/slot/port* **[**-*port2***]} macsec [sci-rx [***hex-num***] [sci-tx] [keychain] [encryption]**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for a specific module.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-10).
admin-state enable	Enables MACsec on a physical port or port range.
admin-state disable	Disables MACsec on a physical port or port range.
static	Sets the SA (secure association) mode to static. This is enabled by default.
dynamic	Sets the SA (secure association) mode to dynamic.
hex-num	The SCI (Secure Channel Identifier) value (up to 8 bytes in length) for Tx and Rx channel in the hexadecimal format (0xhex). The default SCI value is '0' (implicit SCI value).
keychain_id	The keychain ID associated to Tx/Rx channel.
encryption	Enable or disable the encryption option on the Tx/Rx channel. By default, the 'encryption' is disabled.
cak_kc	The keychain ID for Static-CAK (Connectivity Association Key).
priority	Specifies the server priority in the range 0 to 255.
tx_interval	Specifies the transmit interval for MKPDU in the range 2 to 10 seconds.

Defaults

parameter	default
enable | disable	enable
priority	5, 10, 15, and 15 respectively on OmniSwitch 9900, OmniSwitch 6860, OmniSwitch 6465, and OmniSwitch 6560. *Note: Lower the priority value, higher the precedence.*
tx_interval	2 seconds
encryption	disabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 9900

Usage Guidelines

- Use this command to,
  - Enable or disable MACsec on a physical port or port range.
  - Set the MACsec mode: Static SA Mode or Dynamic SA Mode
- For Static SA Mode - MACsec with Static Secure Association Key (static-SAK), following configurations can be configured:
  - Set the MACsec mode to Static.
  - Create MACsec Tx and Rx channels.
  - Specify the SCI value for Tx and Rx channels.
  - Associate the keychain ID for Tx and Rx channel. For more information on keychain configuration, refer to the “Chassis Management and Monitoring Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.
  - Enable or disable encryption on Tx and Rx channel (optional).
- Dynamic SA Mode has two variations - Dynamic SAK using pre-shared keys and Dynamic SAK using Extensible Authentication Protocol (EAP).
  - For Dynamic SAK using pre-shared keys, following configurations can be configured:
    - > Set the MACsec mode to Dynamic.
    - > Configure the keychain for Static-CAK. For more information on keychain configuration, refer to the “Chassis Management and Monitoring Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.
    - > Configure key server priority (optional).
    - > Configure transmit interval for MKPDUs (optional).
    - > Enable or disable encryption on dynamic secure channel (optional).
  - For Dynamic SAK using EAPs, the following configurations can be configured:
    - > Set the MACsec mode to Radius.
    - > Configure transmit interval for MKPDUs (optional).
    - > Enable or disable encryption on dynamic secure channel (optional).

- By default, the MACsec mode is set to ‘static’. For static mode configuration, manually configured SA keys are used to secure traffic on the point-to-point link between two nodes. For MACsec mode ‘static’, following are the configuration guidelines:
  - Only one Tx and one Rx channel can be configured per interface.
  - Each node that expects to receive traffic sent in a particular transmit secure channel must configure a 'matching' receive secure channel, with an SCI corresponding to the SCI of the transmit secure channel of the peer. MACsec supports one secure channel for Tx and one secure channel for Rx configuration on an interface.
  - The secure channel for both Tx and Rx on an interface can be configured with SCI value of 8 bytes long. It can be provided in short form (that is, 0x01) or full form (0x0000000000000001). 0x00 (all zeros) and 0xFFFFFFFFFFFFFFFF SCI value are not valid.
  - The secure channel for both Tx and Rx on an interface can be configured without specifying a SCI value. In this case, the default value will be considered.
  - The keychain associated with the SCI-Tx and SCI-Rx must have four keys supporting ‘AES-GCM-128’ algorithm, and the number of keys in the keychain associated with both SCI-Tx and SCI-Rx on an interface must be equal.
  - Addition/deletion of keys to/from a keychain already associated with a SCI-Tx and SCI-Rx under MACsec would not be allowed by Security Keychain module. The keychain also cannot be deleted.
  - MACsec cannot be administratively enabled on an interface until both SCI-Tx and SCI-Rx are configured on the interface.
  - The Tx/Rx secure channel cannot be removed without disabling MACsec on the interface.
  - The **encryption** option on the Tx/Rx channel can either be enabled or disabled. By default, the ‘encryption’ is disabled. Enabling ‘encryption’ option ensures that the data in the Ethernet frame cannot be viewed by anyone monitoring traffic on the link. Use the **no** form of the command to disable encryption on Tx/Rx channel.
  - MACsec SCI-Tx/SCI-Rx values cannot be updated at run-time. The SCI-Tx/Rx values must be unconfigured and re-configured. Only ‘keychain ID’ and ‘encryption’ parameters can be updated at run-time.
  - During run-time, upon enabling or disabling MACsec on the port, the interface will get re-initialized (interface will be brought down and up), which will result in temporary traffic loss.
  - MACsec mandates specifying SCI-Tx and SCI-Rx value (for configured explicit SCI) while updating its ‘keychain ID’ and ‘encryption’ parameters on an interface.
  - While unconfiguring ‘keychain ID’ and ‘encryption’ parameters on an interface, it is not mandatory to provide MACsec SCI-Tx value, whereas, MACsec mandates specifying SCI-Rx value (for explicit SCI).
- For MACsec mode ‘dynamic’- dynamic SAK using pre-shared keys, following are the configuration guidelines:
  - The keychain or pre-shared key for Static-CAK must have the key mapped to ‘AES-CMAC-128’ algorithm.
  - If there are multiple pre-shared keys configured in the keychain, only the first key would be used for CAK.
  - Key server priority would be in the range 0-255, with lower value having higher precedence.
  - Enabling or disabling Encryption enables or disables encryption on dynamic Secure-Channel (SC).
- For MACsec mode ‘radius’ - dynamic SAK using EAP, following are the configuration guidelines:
  - Dynamic mode using RADIUS server requires the switch end port connecting a host (supplicant) to be enabled with UNP and configured for 802.1x-authentication, and MSK/Key-Name received from Server as part of the authentication. The authentication method must be either EAP-TLS or PEAP authentication framework.
  - The switch end port connecting a host (supplicant) must be enabled with UNP and configured for 802.1x-authentication.

  - The MACsec mode dynamic on UNP is supported in single supplicant mode only, that is, the UNP port can learn only one supplicant on the MACsec enabled interface. Also, there cannot be any non-supplicant learned on the same port.
  - Flushing the supplicant MAC on UNP port would purge the existing MACsec MKA session, and the port would be unsecured until the supplicant is learned again.
  - Re-authentication of supplicant may change the UNP profile or VLAN and the policy applied to the MAC. The existing MACsec session established (if any) would remain intact if the re-authentication results in the same MSK/Key-Name from RADIUS server. Otherwise, the existing MKA session would be purged and a new session is established using the new MSK/Key-Name.
  - Captive portal authentication, BYOD, and LTP (location/time policy) is not supported on MACsec enabled UNP ports.
  - MACsec mode dynamic using ‘radius’ will not be supported on UNP Linkagg.

- MACsec is supported on the following platforms:
  - OmniSwitch 6465
    - All models support MACsec on all ports.
    - OmniSwitch 6465-P28 - supported on all ports, except ports 27 and 28.
  - OmniSwitch 6560
    - OmniSwitch 6560-P24X4/24X4 - supported on 1G ports 1-24
    - OmniSwitch 6560-P48X4/48X4 - supported on 1G ports 1-48. Supports only MACsec mode ‘dynamic’ on ports 49-50 on 1G ports, and on ports 51-52 on 10G ports.
    - OmniSwitch 6560-P48Z16 (part number 904044-90 only) - supported on 1G ports 1-32 and on ports 33-48 on 2.5G ports. Supports only MACsec mode ‘dynamic’ on ports 49-52 on 10G ports.
    - OmniSwitch 6560-X10 - supports only MACsec mode ‘dynamic’ on ports 1-8 on 10G ports.
  - OmniSwitch 6860 and OmniSwitch 6860E
    - All models support MACsec on 10G ports.
    - OmniSwitch 6860-P24 - supported on 1G and 10G ports.
    - OmniSwitch 6860-P24Z8 - supported on 1G and 10G ports (not supported on 2.5G ports).
  - OmniSwitch 9900
    - MACsec is supported on OS99-CMM (4X10G mode only), OS99-GNI-48/P48, OS99-XNI-48/P48/U48, P48Z16.
    - MACsec is not supported on the OS99-CNI-U8, OS99-GNI-U48, and OS99-CMM in 40G mode.
- MACsec must be enabled on all ports (on a per physical port basis) that are part of the same link aggregation.
- MACsec mode cannot be changed if MACsec is already administratively enabled. To change MACsec mode, administratively disable MACsec first.
- Use the **no** form of this command to disable encryption on Tx/Rx channel, remove keychain configuration on Tx/Rx channel, remove Tx/Rx channel.
- To confirm MACsec support on the interface, use the **show interfaces capability** command. MACsec support is listed in the **MACsec Supported** field.

Examples

```
-> interface port 1/1/1 macsec admin-state enable mode static sci-Tx 0x1 key-chain
1 encryption sci-rx 0x1 key-chain 1 encryption
```

```
-> interface port 1/1/1 macsec admin-state enable mode dynamic key-chain 1 server-
priority 10 transmit-interval 3

-> interface port 1/1/1 macsec admin-state enable mode dynamic radius

-> no interface port 1/1/1 macsec sci-rx 0x2 keychain
-> no interface port 1/1/1 macsec sci-tx encryption
```

Release History

Release 8.4.1 R03; command introduced.
Release 8.5R2; Dynamic SA Mode - Dynamic SAK using Pre-Shared Key and Dynamic SAK using EAP support added.

Related Commands

show interfaces macsec	Displays the MACsec configuration on a physical port or port range.
show interfaces macsec static	Displays the detailed MACsec configuration on a physical port or port range configured with MACsec mode ‘Static.
show interfaces macsec dynamic	Displays the detailed MACsec configuration on a physical port or port range configured with MACsec mode ‘Dynamic’.
show interfaces macsec statistics	Displays the MACsec statistics collected for a physical port.

MIB Objects

```
alaSecyTxSCTable
   alaSecyTxSCI
   alaSecyTxSCKeyChainId
   alaSecyTxSCEncryption
alaSecyRxSCTable
   alaSecyRxSCI
   alaSecyRxSCKeyChainId
   alaSecyRxSCEncryption
alaSecyIfTable
   alaSecyIfAdminStatus
   alaSecyIfMode
```

show interfaces macsec

Displays the MACsec configuration on a physical port or port range.

show interfaces macsec [*chassis/slot/port* **[-***port2***]**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

By default, the MACsec configuration on all ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 9900

Usage Guidelines

Enter a port number with this command to display the MACsec configuration for a specific port.

Examples

```
-> show interfaces macsec
Chas/Slot/Port   Admin-State     Mode          Encryption
---------------+-------------+------------+-----------------
     1/1/1       Enabled        Static         Enabled
     1/1/2       Disabled       Static         Disabled
     1/1/3       Disabled       Static         TX Enabled
     1/1/3       Disabled       Static         RX Enabled
     1/1/4       Enabled        Dynamic        Enabled
     1/1/5       Enabled        Dynamic        Disabled

-> show interfaces macsec 1/1/1
 Chas/Slot/Port  Admin-State     Mode          Encryption
---------------+-------------+------------+-----------------
     1/1/1       Enabled        Static         Enabled

-> show interfaces macsec 1/1/1-2
 Chas/Slot/Port  Admin-State     Mode          Encryption
---------------+-------------+------------+-----------------
     1/1/1       Enabled        Static         Enabled
     1/1/2       Disabled       Static         Disabled
```

output definitions

Chas/Slot/Port	The chassis/slot/port identifier.
Admin-State	The interface administrative status.

output definitions (continued)

Mode	The MACsec mode.
Encryption	Status of encryption on Tx/Rx channel. Encryption field will display "Enabled" or "Disabled" if it is enabled or disabled respectively on both Tx/Rx. However, if encryption is enabled only on Tx or only on Rx, it would be disabled as "Tx Enabled" or "Rx Enabled" respectively.

Release History

Release 8.4.1.R03; command introduced.

Related Commands

interfaces macsec admin-state	This command enables or disables MACsec on a physical port or a port range.

MIB Objects

```
alaSecyIfTable
   alaSecyIfAdminStatus
   alaSecyIfMode
alaSecyTxSCTable
   alaSecyTxSCEncryption
alaSecyRxSCTable
   alaSecyRxSCEncryption
```

show interfaces macsec static

Displays the detailed MACsec configuration on a physical port or port range configured with MACsec mode ‘Static’.

show interfaces macsec static [*chassis/slot/port* **[-***port2***]**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

By default, the detailed MACsec configuration on all ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 9900

Usage Guidelines

Enter a port number with this command to display the detailed MACsec configuration for a specific port.

Examples

```
-> show interfaces macsec static
 Chas/Slot/Port  Admin-State           SCI          Type   Keychain     Encryption
---------------+-------------+--------------------+------+-----------+-------------
     1/1/1       Enabled       0x0000000000000001   TX        1         Enabled
     1/1/1       Enabled       0x0000000000000002   RX        1         Enabled
     1/1/2       Disabled             -              TX        2         Disabled
     1/1/2       Disabled             -              RX        2         Disabled
     1/1/3       Disabled      0x0000000000000003   TX        3         Enabled
     1/1/3       Disabled      0x0000000000000004   RX        3         Disabled

-> show interfaces macsec static 1/1/1
 Chas/Slot/Port  Admin-State           SCI          Type   Keychain     Encryption
---------------+-------------+--------------------+------+-----------+-------------
     1/1/1       Enabled       0x0000000000000001   TX        1         Disabled
     1/1/1       Enabled       0x0000000000000002   RX        1         Disabled
```

output definitions

Chas/Slot/Port	The chassis/slot/port identifier.
Admin-State	The interface administrative status.
SCI	The configured SCI value for Tx and Rx channel in the hexadecimal format (0xhex).
Type	Specifies the secure channel type: Tx/Rx

output definitions (continued)

Keychain	The keychain ID associated to Tx/Rx channel.
Mode	The MACsec mode.
Encryption	Status of encryption on Tx/Rx channel.

Release History

Release 8.4.1 R03; command introduced.

Related Commands

interfaces macsec admin-state	This command enables or disables MACsec on a physical port or a port range.

MIB Objects

```
alaSecyTxSCTable
   alaSecyTxSCI
   alaSecyTxSCKeyChainId
   alaSecyTxSCEncryption
alaSecyRxSCTable
   alaSecyRxSCI
   alaSecyRxSCKeyChainId
   alaSecyRxSCEncryption
alaSecyIfTable
   alaSecyIfAdminStatus
   alaSecyIfMode
```

show interfaces macsec dynamic

Displays the detailed MACsec configuration on a physical port or port range configured with MACsec mode ‘Dynamic’.

show interfaces macsec dynamic [details] [*chassis/slot/port* **[-***port2***]**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

By default, the detailed MACsec configuration on all ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 9900

Usage Guidelines

Enter a port number with this command to display the detailed MACsec configuration for a specific port.

Examples

```
-> show interface macsec dynamic
                                                        Server     Transmit        Key     Operation
 Chas/Slot/Port   Admin-State   Mode       Keychain   Encryption   Priority   Interval(Sec)   Server   Status
----------------+-------------+----------+----------+------------+----------+---------------+--------+---------
 1/1/1            Enabled       keychain    2         Enabled        10         3             YES      UP
 1/1/3            Enabled       keychain    1         Disabled       12         2             YES      UP
 1/1/4            Enabled       keychain    1         Disabled       13         5             NO       UP
 1/1/5            Enabled       radius      NA        Disabled       14         6             NO       UP


-> show interface macsec dynamic 1/1/3-4
                                                        Server     Transmit        Key     Operation
 Chas/Slot/Port   Admin-State   Mode       Keychain   Encryption   Priority   Interval(Sec)   Server   Status
----------------+-------------+----------+----------+------------+----------+---------------+--------+--------
 1/1/3            Enabled       keychain    1         Disabled       12         2             YES      UP
 1/1/4            Enabled       keychain    1         Disabled       13         5             NO       UP


-> show interface macsec dynamic 1/1/5
                                                        Server     Transmit        Key     Operation
 Chas/Slot/Port   Admin-State   Mode       Keychain   Encryption   Priority   Interval(Sec)   Server   Status
 ----------------+-------------+----------+----------+------------+----------+---------------+--------+--------
 1/1/5            Enabled       radius      NA        Disabled       14         6             NO       UP
```

```
-> show interfaces macsec dynamic details 1/1/3-4

 Chas/Slot/Port     SCI                    Type          In-used SA       PN
---------------+--------------------+----------+------------------+------------
      1/1/3      0x0000000000000001      TX               0           10
      1/1/3      0x0000000000000002      RX               1           50
      1/1/4      0x0000000000000003      TX               0           20
```

```
      1/1/4      0x0000000000000004      RX              1           30
      1/1/5      0x0000000000000005      TX              0           40
      1/1/5      0x0000000000000006      RX              1           50

-> show interfaces macsec dynamic details 1/1/4

 Chas/Slot/Port     SCI                 Type         In-use SA       PN
---------------+--------------------+----------+-----------------+------------
      1/1/4      0x0000000000000003      TX             0            20
      1/1/4      0x0000000000000004      RX             1            30
```

output definitions

Chas/Slot/Port	The chassis/slot/port identifier.
Admin-State	The interface administrative status.
Mode	The MACsec mode. ‘Keychain’, ‘Radius’ keyword denotes dynamic MACsec using pre-shared key or EAP (RADIUS server) respectively.
Keychain	The keychain ID associated to Tx/Rx channel.
Encryption	Status of encryption on Tx/Rx channel.
Server Priority	The priority configured for the key server.
Transmit Interval(Sec)	The transmit interval configured for MKPDU (in seconds).
Key Server	Indicates the key server.
Operation Status	The MACsec operational status.
SCI	The SCI value dynamically generated for Tx and Rx channel in the hexadecimal format (0xhex).
Type	Specifies the secure channel type: Tx/Rx.
In-use SA	Identifier for currently active Association Number (SA) in use for Tx/Rx channel on the interface.
PN	The packet number of the last packet received on the MACsec interface.

Release History

Release 8.5R2; command introduced.

Related Commands

interfaces macsec admin-state	This command enables or disables MACsec on a physical port or a port range.

MIB Objects

NA

show interfaces macsec statistics

Displays the MACsec statistics collected for a physical port.

show interfaces macsec statistics [*chassis/slot/port* **[-***port2***]**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

- If chassis/slot/port is not specified, the output will be displayed in tabular format but only important statistics will be displayed.
- If chassis/slot/port is specified, the output will not be displayed in tabular format but all statistics will be displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 9900

Usage Guidelines

N/A

Examples

```
-> show interfaces macsec statistics
Chas/                    TX            TX                          RX             RX
Slot/        Bytes       Untagged      Too-Long      Bytes         Untagged       Bad-Tag
Port         Xmitted     Pkts          Received      Pkts          Pkts           Pkts
---------+------------+-----------+-------------+--------------+--------------+------------
1/1/3          0           0              0           0             0              0
1/1/4          0           0              0           0             0              0

-> show interfaces macsec statistics 1/1/1
Chassis/Slot/Port 1/1/2
  Byte Transmitted     :          21035280,     Untagged TX Pkts     :                0
  Too Long TX Pkts     :                 0,     Byte Received        :                0
  Untagged RX Pkts     :                 0,     No Tagged RX Pkts    :              466
  Bad Tagged RX Pkts   :                 0,     Unknown SCI RX Pkts  :                0
  No SCI RX Pkts       :                 0,     Overrun RX Pkts      :                0
  SCI-TX: 0x0000000000000001
    TX Protected Pkts      :                0,    TX Encrypted Pkts      :               0
    TX Octets Protected    :           487920,    TX Octets Encrypted    :          16340448
      SA: 0
        TX Protected Pkts      :     10165,    TX Encrypted Pkts      :    340427
      SA: 1
        TX Protected Pkts      :         0,    TX Encrypted Pkts      :         0
  SCI-RX: 0x0000000000000002
    RX Unused SA Pkts      :                0,    RX No Using SA Pkts    :               0
    RX Late Pkts           :                0,    RX Not Valid Pkts      :               0
```

```
RX Invalid Pkts        :                0,    RX Delayed Pkts        :                0
RX Unchecked Pkts      :                0,    RX OK Pkts             :                0
RX Octets Validated    :                0,    RX Octets Decrypted    :                0
  SA: 0
    RX Unused SA Pkts      :         0,    RX No Using SA Pkts     :         0
    RX Not Valid Pkts      :         0,    RX Invalid Pkts         :         0
    RX OK Pkts             :         0
  SA: 1
    RX Unused SA Pkts      :         0,    RX No Using SA Pkts     :         0
    RX Not Valid Pkts      :         0,    RX Invalid Pkts         :         0
    RX OK Pkts             :         0s...
```

output definitions

Chas/Slot/Port	Interface chassis, slot and port.
Bytes Xmitted	Number of Bytes transmitted.
TX Untagged Pkts	Number of untagged packets transmitted.
TX Too-Long Pkts	Number of long packets transmitted.
Bytes Received	Number of Bytes received.
RX Untagged Pkts	Number of untagged packets received.
RX Bad-Tag Pkts	Number of bad tag packets received.
Unknown SCI RX Pkts	Number of unknown packets received.
Overrun RX Pkts	Number of packets overrun.
TX Protected Pkts	Number of protected packets transmitted.
TX Encrypted Pkts	Number of encrypted packets transmitted.
TX Octets Protected	Number of packets protected in each listed octet range.
TX Octets Encrypted	Number of packets encrypted in each listed octet range.
RX Unused SA Pkts	Number of unused SA packets received.
RX No Using SA Pkts	Number of SA packets not used.
RX Late Pkts	Number of late packets received.
RX Not Valid Pkts	Number of discarded packets.
RX Invalid Pkts	Number of invalid packets.
RX Delayed Pkts	Number of delayed packets received.
RX Unchecked Pkts	Number of unchecked packets received.
RX OK Pkts	Number of valid packets.
RX Octets Validated	Number of packets validated in each listed octet range.
RX Octets Decrypted	Number of packets decrypted in each listed octet range.

Release History

Release 8.4.1 R03; command introduced.

Related Commands

interfaces macsec admin-state	This command enables or disables MACsec on a physical port or a port range.

MIB Objects

```
secyTxSAStatsTable
   secyTxSAStatsProtectedPkts
   secyTxSAStatsEncryptedPkts
secyTxSCStatsTable
   secyTxSCStatsProtectedPkts
   secyTxSCStatsEncryptedPkts
   secyTxSCStatsOctetsProtected
   secyTxSCStatsOctetsEncrypted
secyRxSAStatsTable
   secyRxSAStatsUnusedSAPkts
   secyRxSAStatsNoUsingSAPkts
   secyRxSAStatsNotValidPkts
   secyRxSAStatsInvalidPkts
   secyRxSAStatsOKPkts
secyRxSCStatsTable
   secyRxSCStatsUnusedSAPkts
   secyRxSCStatsNoUsingSAPkts
   secyRxSCStatsLatePkts
   secyRxSCStatsNotValidPkts
   secyRxSCStatsInvalidPkts
   secyRxSCStatsDelayedPkts
   secyRxSCStatsUncheckedPkts
   secyRxSCStatsOKPkts
   secyRxSCStatsOctetsValidated
   secyRxSCStatsOctetsDecrypted
secyStatsTable
   secyStatsTxUntaggedPkts
   secyStatsTxTooLongPkts
   secyStatsRxUntaggedPkts
   secyStatsRxNoTagPkts
   secyStatsRxBadTagPkts
   secyStatsRxUnknownSCIPkts
   secyStatsRxNoSCIPkts
   secyStatsRxOverrunPkts
```

clear interfaces macsec statistics

Clears the MACsec statistics globally on all MACsec enabled interfaces.

clear interfaces {slot *chassis/slot* **| port [***chassis/slot/port* **[-***port2***] |all} macsec-statistics**

Syntax Definitions

chassis	The chassis identifier.
slot	Slot number to display information about all ports on a specific slot.
*port***[-***port2***]**	The port number of a specific interface to display. Use a hyphen to specify a range of ports.
all	Displays information on all MACsec enabled interfaces.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 9900

Usage Guidelines

This command is used to clear MACsec statistics on a slot, port, port-range, or on all interfaces globally.

Examples

```
-> clear interface port 1/1/1 macsec-statistics
-> clear interface port 1/1/1-2 macsec-statistics
-> clear interface slot 1/1 macsec-statistics
-> clear interface all macsec-statistics
```

Release History

Release 8.4.1 R03; command introduced.
Release 8.5 R1; **all** keyword added.

Related Commands

interfaces macsec admin-state	This command enables or disables MACsec on a physical port or a port range.

MIB Objects

```
alaSecyIfTable
   alaSecyIfPortClearStats
```

2 Power over Ethernet (PoE) Commands

The Power over Ethernet (PoE) feature is supported on OmniSwitch PoE-capable switches. Refer to the *OmniSwitch Hardware Users Guide* for further details.

Note on Terminology. There are several general terms used to describe this feature. The terms *Power over Ethernet (PoE), Power over LAN (PoL), Power on LAN (PoL),* and *Inline Power* are synonymous terms used to describe the powering of attached devices via Ethernet ports. For consistency, this chapter and the *OmniSwitch AOS Release 8 CLI Reference Guide* refer to the feature as *Power over Ethernet (PoE).*

Additional terms, such as *Powered Device (PD)* and *Power Source Equipment (PSE)* are terms that are not synonymous, but are directly related to PoE.

- *PD* refers to any attached device that uses a PoE data cable as its only source of power. Examples include access points such as IP telephones, Ethernet hubs, wireless LAN stations, etc.
- *PSE* refers to the actual hardware source of the electrical current for PoE (e.g., OmniSwitch PoE-capable switches.

PoE commands documented in this section comply with IEEE 802.3, 802.af, and 802.3at.

MIB information for the PoE commands is as follows:

Filename: ALCATEL-IND1-INLINE-POWER-MIB.mib
Module: alcatelIND1INLINEPOWERMIB

Filename: POWER-ETHERNET-MIB.mib
Module: powerEthernetMIB

A summary of the available commands is listed here:

lanpower service
lanpower port admin-state
lanpower type
lanpower power
lanpower maxpower
lanpower priority
lanpower ni-priority
lanpower priority-disconnect
lanpower power-rule
lanpower power-policy
lanpower class-detection
lanpower capacitor-detection
lanpower usage-threshold
lanpower dynamic-power-mgmt
lanpower update-from
lanpower 4pair
lanpower power-over-hdmi
lanpower 802.3bt
show lanpower slot
show lanpower power-rule
show lanpower power-policy
show lanpower class-detection
show lanpower capacitor-detection
show lanpower priority-disconnect
show lanpower ni-priority
show lanpower usage-threshold
show lanpower update-from

lanpower service

Activates or stops PoE service on all ports in a specified slot.

lanpower {chassis *chassis* **| slot** *chassis/slot* **} service {start | stop}**

Syntax Definitions

chassis	The chassis on which the PoE power is being turned on or off.
chassis/slot	The slot on which the PoE power is being turned on or off.
start	Activates PoE on all ports in the specified slot.
stop	Turns off PoE on all ports in the specified slot.

Defaults

Power over Ethernet is globally disabled by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

The OmniSwitch 6465 cannot auto-detect the type of power supply connected. The type of power supply connected must be configured so that the system and PoE power information is correctly displayed and utilized. Use the **powersupply type** type command to configure the power supply.

Examples

```
-> lanpower slot 2/1 service start
-> lanpower chassis 1 service stop
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower port admin-state	Activates or stops PoE service on an individual port.
lanpower update-from	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPseAdminStatus
```

lanpower port admin-state

Activates or stops PoE service on an individual port.

lanpower port *chassis/slot/port* **admin-state {enable | disable}**

Syntax Definitions

chassis/slot/port	The individual port on which the PoE power is being turned on or off.
enable	Activates PoE on the specified port.
stop	Turns off PoE on the specified port.

Defaults

Power over Ethernet is globally disabled by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

N/A

Examples

```
-> lanpower port 2/1/1 admin-state enable
-> lanpower port 1/1/12 admin-state disable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

lanpower service	Activates or stops PoE service on all ports in a specified slot.
lanpower update-from	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
pethPsePortTable
   pethPsePortAdminEnable
```

lanpower type

Assigns a user-defined port type to a specific port (when *chassis/slot/port* values are entered) or across all ports in a chassis or slot.

lanpower {chassis *chassis* | **slot** *chassis/slot* | **port** *chassis/slot/port***} type** *string*

Syntax Definitions

chassis	The chassis on which a port type is being defined.
chassis/slot	The slot on which a port type is being defined.
chassis/slot/port	The specific port on which a port type is being defined.
string	A user-defined text string of up to nine (9) characters. This text string will be listed in the "Type" column in the **lanpower update-from** command output.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

N/A

Examples

```
-> lanpower slot 1/1 type test
-> lanpower port 1/1/23 type PDs
-> lanpower chassis 1 type test
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower update-from	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
pethPsePortTable
   pethPsePortType
```

lanpower power

Specifies the amount of power, in milliwatts, provided for a specific port (when *chassis/slot/port* values are entered) or across all ports in a chassis or slot.

lanpower {chassis *chassis* | **slot** *chassis/slot* | **port** *chassis/slot/port***} power** *milliwatts*

Syntax Definitions

chassis	The chassis on which the port power is being defined.
chassis/slot	The slot on which the port power is being defined.
chassis/slot/port	The specific port on which the port power is being defined.
milliwatts	The maximum amount of power for a specified port or slot. Refer to default and range information below.

Defaults

Refer to the *OmniSwitch Hardware Users Guide* for default power settings.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- Using this command does not immediately allocate the power to the slot or port. Any unused power is still available and remains a part of the overall PoE budget.
- To globally specify the amount of inline power available to all ports in a slot, refer to the **lanpower maxpower** command on page 2-8.
- Be sure that the value specified complies with specific power requirements for all attached PDs.
- Note that the power value for the **lanpower power** command is specified in milliwatts (mW); the related command, **lanpower maxpower**, is specified in watts (W).

Examples

```
-> lanpower slot 3/1 power 3200
-> lanpower port 1/1/24 power 25000
-> lanpower chassis 1 power 3000
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower maxpower	Specifies the maximum amount of inline power, in watts, available to all PoE ports in a specified slot.
lanpower update-from	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
alaPethPsePortTable
   alaPethPsePortPowerMaximum
```

lanpower maxpower

Specifies the maximum amount of power, in watts, assigned to a specified slot.

lanpower {chassis *chassis* | **slot** *chassis/slot* **} maxpower** *watts*

Syntax Definitions

chassis	The chassis containing PoE ports on which the maximum amount of inline power allowed is being configured.
chassis/slot	The slot containing PoE ports on which the maximum amount of inline power allowed is being configured.
watts	The maximum amount of inline power, in watts, available to all PoE ports in the corresponding slot. Refer to the *OmniSwitch Hardware Users Guide* for additional PoE specifications.

Defaults

installed power supply	default	range
920W Power Supply (OS6860)	780W	37-780
600W Power Supply (OS6860)	450W	37-450

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- To specify the maximum amount of inline power available to a single port, refer to the **lanpower power**.
- Note that the power value for the **lanpower maxpower** command is specified in watts (W); the related command, **lanpower power**, is specified in milliwatts (mW).

Examples

```
-> lanpower slot 3/1 maxpower 400
-> lanpower chassis 1 maxpower 400
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower power	Specifies the amount of power, in milliwatts, provided for a specific port (when *chassis/slot/port* values are entered) or across all ports in a slot (if only *slot/port* values are entered).
lanpower update-from	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPseMaxPower
```

lanpower priority

Specifies PoE power priority level to a port (when *chassis/slot/port* values are entered) or across all ports in a slot (if only *slot/port* values are entered). Levels include critical, high, and low.

lanpower {chassis *chassis* | **slot** *chassis/slot* | **port** *chassis/slot/port***} priority {critical | high | low}**

Syntax Definitions

chassis	The chassis on which the PoE power priority is being set.
chassis/slot	The slot on which the PoE power priority is being set.
chassis/slot/port	The specific port on which the PoE power priority is being set.
critical	Intended for ports that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, power to critical ports is maintained as long as possible.
high	Intended for ports that have important, but not mission-critical, devices attached. If other ports in the chassis have been configured as critical, power to high-priority ports is given second priority to critical devices.
low	Intended for ports that have low-priority devices attached. In the event of a power management issue, power to low-priority ports is interrupted first (i.e., before critical- and high-priority ports).

Defaults

parameter	default
low | high | critical	low

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power. For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power.

Examples

```
-> lanpower slot 2/1 priority low
-> lanpower port 1/1/6 priority critical
-> lanpower chassis 1 priority low
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower priority-disconnect	Enables or disables the priority disconnect function on all ports in a specified slot.
lanpower update-from	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
pethPsePortTable
   pethPsePortPowerPriority
```

lanpower ni-priority

Specifies power priority level to a Network Interface (NI) module. Levels include critical, high, and low.

lanpower {chassis *chassis* | **slot** *chassis/slot* **} ni-priority {critical | high | low}**

Syntax Definitions

chassis	The chassis on which the NI priority is being set.
chassis/slot	The slot on which the NI priority is being set.
critical	Intended for modules that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, power to critical NIs is maintained as long as possible.
high	Intended for modules that have important, but not mission-critical, devices attached. If other NIs in the chassis have been configured as critical, power to high-priority modules is given second priority to critical devices.
low	Intended for modules that have low-priority devices attached. In the event of a power management issue, power to low-priority modules is interrupted first (i.e., before critical- and high-priority NIs).

Defaults

parameter	default
low | high | critical	low

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power. For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power.

Examples

```
-> lanpower slot 2/1 ni-priority low
-> lanpower chassis 1 ni-priority low
```

Release History

Release 8.3.1; command was introduced.

Related Commands

show lanpower ni-priority	Displays current Network Interface (NI) modules status for a specified chassis or slot.

MIB Objects

N/A

lanpower priority-disconnect

Enables or disables the priority disconnect function on all ports in a specified slot. Priority disconnect is used by the system software in determining whether an incoming PD will be granted or denied power when there are too few watts remaining in the PoE power budget for an additional device.

lanpower {chassis *chassis* | **slot** *chassis/slot***} priority-disconnect {enable | disable}**

Syntax Definitions

chassis	The chassis on which the priority disconnect function is being enabled or disabled.
chassis/slot	The particular slot on which the priority disconnect function is being enabled or disabled.
enable	Enables priority disconnect on a specified port. When this function is enabled *and* a power budget deficit occurs in which there is inadequate power for an incoming device, the system software uses priority disconnect rules to determine whether an incoming device will be granted or denied power.
disable	Disables priority disconnect on a specified port. When priority disconnect is disabled and there is inadequate power in the budget for an additional device, power will be denied to *any* incoming PD, regardless of its priority status.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power (per power supply installed). For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power (per power supply installed).

Examples

```
-> lanpower slot 2/1 priority-disconnect enable
-> lanpower chassis 1 priority-disconnect disable
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower priority	Specifies PoE power priority level to a port (when *chassis/slot/port* values are entered) or across all ports in a slot (if only *slot/port* values are entered).
lanpower update-from	Displays the PoE status and related statistics for all ports in a specified slot.
show lanpower priority-disconnect	Displays current priority disconnect status for a specified slot.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPsePriorityDisconnect
```

lanpower power-rule

Specifies user-defined power rules that can be assigned to PoE ports.

lanpower power-rule *rule-name* **[admin-state {enable | disable}] [power {on | off}] [at {minutes** *mm* **| time** *hh:mm***}] [days {all |** *day [day...]* **| date** *[date...]***} [months {all |** *month***}] [timezone {local-server | utc | originator-server}]**

no lanpower power-rule *rule-name* **[admin-state {enable | disable}] [power {on | off}] [at {minutes** *mm* **| time** *hh:mm***}] [days {all |** *day [day...]* **| date** *[date...]***} [months {all |** *month***}] [timezone {local-server | utc | originator-server}]**

Syntax Definitions

rule-name	A user-defined name (up to 128 characters) for the power rule being configured.
admin-state	Specifies the admin-state for the power rule.
enable	Enables the power rule.
disable	Disables the power rule.
power	Specifies the power status (**on** or **off**) for devices connected to ports within the power rule.
on	Powers on devices on ports for which the rule is assigned.
off	Powers off devices on ports for which the rule is assigned.
at	Activates a a power rule timer. Power rules are triggered on a specified date or day of the week or at a particular time, or after a specified amount of time has elapsed.
minutes	Sets a timer. Power rules will take effect when a specified number of minutes have elapsed.
mm	The number of minutes that will elapse before the power rules take effect.
time	Sets a timer. Power rules will take effect at a specified time of day.
hh:mm	The time of day that the power rule will take effect.
days	Specifies that the power rule will take effect on a particular day of the week.
all	Specifies that the power rule will take effect on all days of the week (Monday through Sunday).
day	Specifies a particular day of the month or week the power rule will take effect. When entering a day of the month, enter one or more numbers from **1** to **31**. When entering a day of the week, use three-digit abbreviations (e.g., **mon**, **tue**, **wed**, **thu**, **fri**, **sat** and **sun**). Any combination of days may be entered in any order. Refer to command line examples for more information.
month	Specifies that the power rule will take effect during a particular month.
all	Specifies that the power rule will take effect during all months of the year (January through December).

month	Specifies a particular month of the year the power rule will take effect. When entering a month, use three-digit abbreviations (e.g., **jan**, **feb**, **mar**, **apr**, **may**, **jun**, **jul**, **aug**, **sep**, **oct**, **nov** and **dec**). Any combination of months may be entered in any order. Refer to command line examples for more information.
timezone	Sets a timezone in which timer-based power rules will take effect.
local-server	Time as specified by a local server.
utc	Specifies that timer-based rules fall under Universal Time Coordinated (UTC) time.
originator-server	Time as specified via the network.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

Before a power rule can take effect, the rule must first be assigned to particular slots or ports via the **lanpower power-policy** command.

Examples

```
->lanpower power-rule RuleTest2 admin-state enable power on at minutes 10 days fri
thu tue months all timezone utc
-> lanpower power-rule new power on at time 18:30 days all months all timezone utc
->lanpower power-rule OutgoingPDs power off at time 6:00 days 1 2 3 6 9 12 31
months all timezone utc
-> lanpower power-rule NewRule admin-state enable power off at minutes 4 days all
months all timezone utc
```

Release History

Release 8.1.1; command was introduced.

Related Commands

lanpower power-policy	Allows users to bind existing power rules to particular slots or ports.
show lanpower power-rule	Displays current PoE power rule settings.
show lanpower power-policy	Displays existing power policies assigned to a slot, port or rule.

MIB Objects

```
alaPethPowerRuleTable
   alaPethPowerRuleAdminStatus
   alaPethPowerRulePowerStatus
   alaPethPowerRuleAtMinute
   alaPethPowerRuleAtTime
   alaPethPowerRuleDaysOfMonth
   alaPethPowerRuleDaysOfWeek
   alaPethPowerRuleMonths
   alaPethPowerRuleTimezone
   alaPethPowerRuleRowStatus
```

lanpower power-policy

Allows users to bind existing power rules to particular slots or ports.

lanpower [slot *chassis/slot* | **port** *chassis/slot/port-port***] power-policy** *policy-name* **[power-rule** *rule-name***]**

no lanpower power-policy *name*

Syntax Definitions

chassis/slot	The slot on which the power policy (with its associated power rule) is being assigned. This syntax is used the first time the **lanpower power-policy** command is entered, where a policy is being assigned to a particular slot. See Usage Guidelines below for more information.
chassis/slot/port-port	The specific slot on which the power policy (with its associated power rule) is being assigned. Port values may be entered as a single port or range of ports. This syntax is used the first time the **lanpower power-policy** command is entered, where a policy is being assigned to a particular slot. See Usage Guidelines below for more information
policy-name	A user-defined name (up to 128 characters) for the power policy being configured (or assigned to an existing power rule).
rule-name	This syntax is used the second time the **lanpower power-policy** command is entered, where a policy is being assigned to an existing power rule. See Usage Guidelines below for more information.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- One or more power rules must be created before using the **lanpower power-policy** command. For information on creating power rules, see the **lanpower power-rule** command on page 2-16.
- Using the **lanpower power-policy** command is a two-step process. First, use the command to assign the policy to specific slots or ports. For example:

```
-> lanpower slot 1/1 power-policy NewPolicy
-> lanpower port 1/1/23 power-policy NewPolicy
-> lanpower port 1/1/1-12 power-policy NewPolicy
```

  Next, run the command again to assign the policy (with its associated slots or ports) to an existing power rule. For example:

```
-> lanpower power-policy NewPolicy power-rule NewRule
```

- When assigning a policy to a slot or port, be sure to use the syntax, **"slot"** or **"port",** before the *chassis/slot* or *chassis/slot/port* values in the command line. Refer to the examples below for more information.

Examples

```
-> lanpower slot 1/1 power-policy NewPolicy
-> lanpower port 1/1/23 power-policy NewPolicy
-> lanpower power-policy NewPolicy power-rule NewRule
-> no lanpower power-policy NewPolicy
```

Release History

Release 8.1.1; command was introduced.

Related Commands

lanpower power-rule	Specifies user-defined power rules that can be assigned to PoE ports.
show lanpower power-rule	Displays current PoE power rule settings.
show lanpower power-policy	Displays existing power policies assigned to a slot, port or rule.

MIB Objects

```
alaPethPowerPolicyTable
   alaPethPowerPolicyRowStatus
alaPethPowerPortTable
   alaPethPowerPortPolicyName
   alaPethPowerPortRowStatus
```

lanpower class-detection

Enables or disables class detection of attached devices. When class detection is enabled, attached devices will automatically be limited to their class power, regardless of port power configuration.

lanpower {chassis *chassis* | **slot** *chassis/slot***} class-detection {enable | disable}**

Syntax Definitions

chassis	The chassis on which class detection is being enabled or disabled.
chassis/slot	The particular slot on which class detection is being enabled or disabled.
enable	Enables class detection on the specified slot.
disable	Disables class detection on the specified slot.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- Although class-detection is disabled by default, the OmniSwitch 6860 still provides power to incoming PDs (if available in the power budget). However, to strictly enforce class detection as specified in the 802.3at standard, class detection must be enabled using the **lanpower slot class-detection** command.
- Enabling class detection will reset all PoE ports on the chassis.

Examples

```
-> lanpower slot 1/1 class-detection enable
-> lanpower chassis 1 class-detection disable
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

show lanpower class-detection	Displays class detection status on a specified slot.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPseClassDetection
```

lanpower capacitor-detection

Enables or disables the capacitor detection method.

lanpower {chassis *chassis* | **slot** *chassis/slot***} capacitor-detection {enable | disable}**

Syntax Definitions

chassis	The chassis on which class detection is being enabled or disabled.
chassis/slot	The particular slot on which class detection is being enabled or disabled.
enable	Enables the capacitor detection method on the specified slot.
disable	Disables the capacitor detection method on the specified slot.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

The capacitor detection method should only be enabled if there are legacy IP phones attached to the corresponding slot—this feature is *not* compatible with IEEE specifications. Please contact your Alcatel-Lucent Enterprise sales engineer or Customer Support representative to find out which Alcatel-Lucent Enterprise IP phones models need capacitive detection enabled.

Examples

```
-> lanpower slot 3/1 capacitor-detection enable
-> lanpower chassis 1 capacitor-detection disable
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

show lanpower capacitor-detection	Displays capacitor detection status on a specified slot.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPseCapacitorDetect
```

lanpower usage-threshold

Tells the switch to watch for a user-defined, slot-wide threshold for PoE power usage, in percent. When the usage threshold is reached or exceeded, a notification is sent to the user.

lanpower {chassis *chassis* | **slot** *chassis/slot***} usage-threshold** *num*

Syntax Definitions

chassis	The chassis for which usage threshold monitoring is being set.
chassis/slot	The slot for which usage threshold monitoring is being set.
num	The percentage of allowed usage from attached PoE devices before a notification is sent to the user.

Defaults

parameter	default
num	99

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

The **lanpower slot usage-threshold** does not affect the amount of PoE power allocated to a particular slot. The command is a monitoring method that tells the switch to send a “specified usage exceeded” notification (i.e., trap) only when a specified percentage has been reached.

Examples

```
-> lanpower slot 1/1 usage-threshold 50
-> lanpower chassis 1 usage-threshold 99
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

show lanpower usage-threshold	Displays current usage threshold, in percent.

MIB Objects

```
pethMainPseTable
   pethMainPseUsageThreshold
```

lanpower dynamic-power-mgmt

Enables dynamic power management for a chassis or slot.

lanpower {chassis *chassis* | **slot** *chassis/slot***} dynamic-power-management {enable | disable}**

Syntax Definitions

chassis	The chassis on which dynamic power management is being enabled or disabled.
chassis/slot	The particular slot on which dynamic power management is being enabled or disabled.
enable	Enables dynamic power management on the specified chassis or slot.
disable	Disables dynamic power management on the specified chassis or slot.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 9900

Usage Guidelines

- Enabling this feature allows the unused allocated PoE power of an NI to be allocated to other NIs.
- Slot ranges are supported in the command line syntax.

Examples

```
-> lanpower slot 1/1 dynamic-power-mgmt enable
-> lanpower chassis 1 dynamic-power-mgmt disable
```

Release History

Release 8.3.1; command was introduced.

MIB Objects

N/A

lanpower update-from

This command is used to update the PoE microcontroller firmware.

lanpower slot {*chassis/slot* | **all}** **update-from** *filename*

Syntax Definitions

chassis/slot	The slot to be updated.
all	Update all the chassis in a virtual chassis.
filename	The file name of the PoE firmware.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- The binary file must be placed in the ***/flash*** directory of the Master.
- Once started, console messages will be displayed during the update procedure which may take up to 10 minutes.
- The lanpower service must be disabled during the update and minimal load should be placed on the switch. The update process must be allowed to finish prior to unplugging or configuring the units.

Examples

```
-> lanpower slot 1/1 update-from poe_binary_version.bin
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show lanpower update-from	Displays current PoE firmware update status.

MIB Objects

N/A

lanpower 4pair

This command is used to configure 2-pair or 4-pair PoE mode.

lanpower {slot *chassis/slot* | **port** *chassis/slot/port-port*} **4pair {enable | disable}**

Syntax Definitions

chassis/slot	The slot on which to configure the PoE mode.
chassis/slot/port-port	The port(s) on which to configure the PoE mode.

Defaults

parameter	default
enable | disable	enabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- This command is applicable for 4-pair high power PoE ports to deliver 60 watts or more.
- When 4-pair mode is enabled the switch will consider Alt-A and Alt-B pairs for PoE.
- When 4-pair mode is disabled the switch will only consider Alt-A pairs for PoE.
- When 4-pair mode is disabled the maximum PoE power for the port is 30W.

Examples

```
-> lanpower slot 1/1 4pair enable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

show lanpower slot	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
alaPethMainPseTable
   alaPethPsePort4PairStatus
```

lanpower power-over-hdmi

This command is used to configure power over HDMI (PoH).

lanpower {slot *chassis/slot* | **port** *chassis/slot/port-port*} **power-over-hdmi {enable | disable}**

Syntax Definitions

chassis/slot	The slot on which to configure PoH.
chassis/slot/port-port	The port(s) on which to configure PoH.

Defaults

parameter	default
enable | disable	OS6860E-P24Z8 - enabled All other platforms - disabled

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- This command is only support on OS6860E models and only on 4-pair HPoE ports.
- This command is used for supporting IEEE802.3bt specific Aruba AP5xx access points on OS6860E 4-pair ports.

Examples

```
-> lanpower slot 1/1 power-over-hdmi enable
-> lanpower port 1/1/1 power-over-hdmi enable
```

Release History

Release 8.6R2; command was introduced.

Related Commands

show lanpower slot	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
alaPethPowerPortTable
   alaPethPsePortPowerOverHdmi
```

lanpower 802.3bt

This command is used to enable IEEE 802.3bt functionality.

lanpower {slot *chassis/slot*} **802.3bt {enable | disable}**

Syntax Definitions

chassis/slot	The slot on which to enable or disable 802.3bt.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6560

Usage Guidelines

- This command can only be executed when the lanpower service is stopped.
- Only applicable on a slot basis, 802.3bt cannot be configured on individual ports.

Examples

```
-> lanpower slot 1/1 802.3bt enable
```

Release History

Release 8.6R2; command was introduced.

Related Commands

show lanpower slot	Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

```
alaPethMainPseTable
   alapethMainPseDot3bt
```

show lanpower slot

Displays the PoE status and related statistics for all ports in a specified slot.

show lanpower slot *chassis/slot*

Syntax Definitions

chassis	The virtual chassis ID for which current inline power status and related statistics are to be displayed.
slot	The slot for which current inline power status and related statistics are to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

N/A

Examples

```
-> show lanpower slot 1/1
Port Maximum(mW) Actual Used(mW)   Status    Priority   On/Off   Class   Type
----+-----------+---------------+-----------+---------+--------+-------+----------
  1     60000            0       Powered Off    Low      OFF       .
  2     60000            0       Powered Off    Low      OFF       .
  3     60000            0       Powered Off    Low      OFF       .
  4     60000            0       Powered Off    Low      OFF       .
  5     30000            0       Powered Off    Low      OFF       .
  6     30000            0       Powered Off    Low      OFF       .
  7     30000            0       Powered Off    Low      OFF       .
  8     30000            0       Powered Off    Low      OFF       .
  9     30000            0       Powered Off    Low      OFF       .
 10     30000            0       Powered Off    Low      OFF       .
...
 45     30000            0       Powered Off    Low      OFF       .
 46     30000            0       Powered Off    Low      OFF       .
 47     30000            0       Powered Off    Low      OFF       .
 48     30000            0       Powered Off    Low      OFF       .

ChassisId 1 Slot 1 Max Watts 780
0 Watts Total Power Budget Used
750 Watts Total Power Budget Available
1 Power Supplies Available
BPS power: Not Available
```

output definitions

Port	A PoE port for which current status and related statistics are being displayed.
Maximum (mW)	The current maximum amount of power available to the corresponding PoE port, in milliwatts. For more information on this parameter, including default values and changing the settings, refer to the **lanpower power** command.
Actual Used (mW)	The actual amount of power being used by an attached device (if applicable), in milliwatts. If no device is attached to the corresponding port, this row displays a value of 0.
Status	Displays the port's current operational status. Options include **Powered On**, **Powered Off**, **Searching**, **Fault**, **Deny** and **Test**. **Powered On** indicates that PoE power activation is complete and the attached device is receiving power. **Powered Off** indicates that no PoE device is attached and/or the port is not receiving PoE power. **Searching** indicates that PoE activation has started and a powered device PD has been detected, but activation or class detection is incomplete. **Fault** indicates that PoE activation or class detection has failed. **Deny** indicates that PoE power management has denied power to the port due to priority disconnect or over subscription. **Test** indicates that the port has been forced on and will remain on until it is forced off by RTP functions.
Priority	The current priority level for the corresponding PoE port. Options include **Critical**, **High**, and **Low**. **Critical** should be reserved for ports that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, inline power to critical ports is maintained as long as possible. **High** indicates ports that have important, but not mission-critical, devices attached. If other ports in the chassis have been configured as critical, inline power to high-priority ports is given second priority. **Low** priority is for ports that have low-priority devices attached. In the event of a power management issue, inline power to low-priority ports is interrupted first (i.e., before critical and high-priority ports). The default value is Low. Priority levels can be changed using the **lanpower priority** command.
On/Off	Displays whether a port has been manually turned on or off by the user. **ON** indicates that the port has been turned on by the user via the **lanpower service** command. **OFF** is the default value and can also indicate that the port has been turned off by the user via the **lanpower service** command.
Class	PoE class detected on the attached Powered Device. See the **lanpower class-detection** command on page 2-21 for more information.
Type	A user-defined name port type (i.e., text string) for the port. See the **lanpower type** command on page 2-5 for more information.
Max Watts	The maximum watts available to the corresponding slot. The maximum watts value for a slot can be changed using the **lanpower maxpower** command.
Actual Power Consumed	The amount of power being used by attached PoE devices.

output definitions (continued)

Actual Power Budget Remaining	The amount of power budget remaining for PoE. If the total power budget remaining is exceeded, a power error will occur and the switch's chassis management software will begin shutting down power to PoE ports according to their priority levels.
Total Power Budget Available	The total amount of power budget available for PoE.
Power Supplies Available	The number of power supplies currently installed and operating in the switch.
*****	An asterisk indicates a 4-pair PoE port is operating in 2-pair mode.

Release History

Release 8.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaPethPsePortPowerActual
alaPethPsePortPowerMaximum
alaPethPsePortPowerStatus
pethPsePortPowerPriority
pethPsePortAdminEnable
pethPsePortPowerClass
```

show lanpower power-rule

Displays current PoE power rule settings.

show lanpower power-rule [*name***]**

Syntax Definitions

name	The name of an existing power rule.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

Entering the **show lanpower power-rule** command without the *name* string provides top-level information for all existing power rules. To view detailed information for a particular rule (e.g., timer and timezone settings, etc.), specify the *name* string in the command line.

Examples

```
-> show lanpower power-rule
Power-Rule                          Admin-state   Power
-----------------------------------+------------+--------------------
test                                 Disabled      Off


-> show lanpower power-rule test
                Power-Rule                :     test
                Admin-state               :     Disabled
                Power                     :     Off
                At HH:MM                  :     00:00
                Day-of-Week               :     All
                Month-of-Year             :     All
                Timezone                  :     Local
```

output definitions

Power-Rule	The name(s) of existing PoE power rule(s).
Admin-state	The port PoE status assigned to the rule. Refer to page 2-16 for more information.
Power	The PoE power status assigned to the rule. Refer to page 2-16 for more information.
At HH:MM	The time of day the power rule takes effect. Refer to page 2-16 for more information.

output definitions (continued)

Day-of-Week	The day of the week the power rule takes effect. Refer to page 2-17 for more information.
Month-of-Year	The month of year the power rule takes effect.Refer to page 2-17 for more information.
Timezone	The timezone under which the power rule takes effect. Options include **local-server**, **originator-server** and **utc**. Refer to page 2-17 for more information.

Release History

Release 8.1.1; command was introduced.

Related Commands

lanpower power-rule	Specifies user-defined power rules that can be assigned to PoE ports.

MIB Objects

N/A

show lanpower power-policy

Displays existing power policies assigned to a slot, port or rule.

show lanpower power-policy [*policy-name* **slot** | *policy-name* **power-rule** | *policy-name* **port**]

Syntax Definitions

policy-name	The text string for an existing power policy.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

Entering the **show lanpower power-policy** command without the *policy-name* string provides top-level information for all existing policies, including associated power rules (if any). To view detailed information for a particular policy, specify the *policy-name* string in the command line, along with the policy's associated slot, port or rule. See Examples below for additional information.

Examples

```
-> show lanpower power-policy
Power-Policy name                   Power-rules
-----------------------------------+-----------------------------------
Mar25                               RuleTest2

-> show lanpower power-policy Mar25 power-rule
            Power-Policy name             : Mar25
                  Power-rules             : RuleTest2
```

output definitions

Power-Policy name	The names of existing PoE power policies.
Power-rules	The power rules associated with the existing power policies.

Release History

Release 8.1.1; command was introduced.

Related Commands

lanpower power-policy	Allows users to bind existing power rules to particular slots or ports.

MIB Objects

N/A

show lanpower class-detection

Displays class detection status on a specified slot.

show lanpower {chassis *chassis* | **slot** *chassis/slot* **} class-detection**

Syntax Definitions

chassis	The chassis for which class detection is being displayed.
chassis/slot	The slot for which class detection is being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- Although class-detection is disabled by default, the OmniSwitch 6860 still provides power to incoming PDs (if available in the power budget). However, to strictly enforce class detection as specified in the 802.3at standard, class detection must be enabled using the **lanpower slot class-detection** command.
- Enabling class detection will reset all PoE ports on the chassis.

Examples

```
-> show lanpower slot 1/1 class-detection
Class Detection disabled on ChassisId 1 Slot 1
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower class-detection	Enables or disables class detection of attached devices.

MIB Objects

N/A

show lanpower capacitor-detection

Displays capacitor detection status on a specified slot.

show lanpower {chassis *chassis* | **slot** *chassis/slot* **} capacitor-detection**

Syntax Definitions

chassis	The chassis for which capacitor detection is being displayed.
chassis/slot	The slot for which capacitor detection is being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

N/A

Examples

```
-> show lanpower slot 1/1 capacitor-detection
Capacitor Detection disabled on ChassisId 1 Slot 1
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower capacitor-detection	Enables or disables the capacitor detection method.

MIB Objects

N/A

show lanpower priority-disconnect

Displays current priority disconnect status for a specified slot.

show lanpower {chassis *chassis* | **slot** *chassis/slot* **} priority-disconnect**

Syntax Definitions

chassis	The chassis on which priority disconnect status is being displayed.
chassis/slot	The particular slot on which priority disconnect status is being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power (per power supply installed). For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power (per power supply installed).

Examples

```
-> show lanpower slot 1/1 priority-disconnect
Priority Disconnect enabled on ChassisId 1 Slot 1
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower priority-disconnect	Enables or disables the priority disconnect function on all ports in a specified slot.

MIB Objects

N/A

show lanpower ni-priority

Displays current Network Interface (NI) modules status for a specified chassis or slot.

show lanpower {chassis *chassis* | **slot** *chassis/slot* **} ni-priority**

Syntax Definitions

chassis	The chassis on which NI priority is being displayed.
chassis/slot	The particular slot on which NI priority is being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power (per power supply installed). For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power (per power supply installed).

Examples

```
-> show lanpower slot 1/1 priority-disconnect
Priority Disconnect enabled on ChassisId 1 Slot 1
```

Release History

Release 8.3.1; command was introduced.

Related Commands

lanpower ni-priority	Specifies power priority level to a Network Interface (NI) module. Levels include critical, high, and low.

MIB Objects

N/A

show lanpower usage-threshold

Displays current usage threshold, in percent.

show lanpower {chassis *chassis* | **slot** *chassis/slot* **} usage-threshold**]

Syntax Definitions

chassis	The chassis on which priority disconnect status is being displayed.
chassis/slot	The particular slot on which priority disconnect status is being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

N/A

Examples

```
-> show lanpower slot 1/1 usage-threshold
Usage Threshold 99% on ChassisId 1 Slot 1
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower usage-threshold	Sets a slot-wide threshold for PoE power usage, in percent.

MIB Objects

N/A

show lanpower update-from

Displays the PoE firmware update status.

show lanpower slot {*chassis/slot* **| all} update-from**

Syntax Definitions

chassis/slot	Display the update status for a slot.
all	Display the update status for all chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

This command can be used to display the update progress from a remote session such as Telnet or SSH.

Examples

```
-> show lanpower slot all update-from
Tue Apr  8 16:48:16 : lpCmm LanCmm info message:
+++ Reprogramming Sequence Started  0 chassisId 1 slot 1
+++ Reprogramming Sequence Started  0 chassisId 2 slot 1

Tue Apr  8 16:48:19 : lpCmm LanCmm info message:
+++ Controller Memory Sequence Begining 0 chassisId 1 slot 1
+++ Controller Memory Sequence Begining 0 chassisId 2 slot 1

Tue Apr  8 16:48:33 : lpCmm LanCmm info message:
+++ Controller Memory Please Wait... 0 chassisId 1 slot 1
+++ Controller Memory Please Wait... 0 chassisId 2 slot 1

Tue Apr  8 16:52:22 : lpCmm LanCmm info message:
+++ Reprogram Pass 0 chassisId 1 slot 1
+++ Reprogram Pass 0 chassisId 2 slot 1
```

Release History

Release 8.1.1; command was introduced.

Related Commands

lanpower update-from	This command is used to update the PoE microcontroller firmware.

MIB Objects

N/A

3 UDLD Commands

This chapter describes the CLI commands used to configure the UDLD (UniDirectional Link Detection) protocol. UDLD operates at Layer 2 in conjunction with IEEE 802.3 Layer 1 fault detection mechanism. It is a protocol used for detecting and disabling unidirectional Ethernet fiber or copper connections to avoid interface malfunctions, Spanning Tree loops, media faults, and so on. It operates in two main modes normal and aggressive.

The two basic mechanisms that UDLD follows are:

- Advertises port identity and learns about its neighbors. This information is maintained in a cache table.
- It sends continuous echo messages when fast notifications are required.

MIB information for the UDLD commands is as follows:

Filename: ALCATEL-IND1-UDLD-MIB.mib
Module: alcatelIND1UDLDMIB

A summary of available commands is listed here:

Configuration procedures for UDLD are explained in "Configuring UDLD," *OmniSwitch AOS Release 8 Network Configuration Guide*.

udld

Globally enables or disables UDLD protocol on the switch.

udld {enable | disable}

Syntax Definitions

enable	Globally enables UDLD on the switch.
disable	Globally disables UDLD on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Auto-negotiation should be disabled on both ends of the link for UDLD to operate properly.
- The port shutdown by this command can be reset by using the **interfaces admin** command.

Examples

```
-> udld enable
-> udld disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

udld port	Enables or disables UDLD status on a specific port or a range of ports.
show udld configuration	Displays the global status of UDLD configuration.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldGlobalStatus
   alaUdldGlobalConfigUdldStatus
```

udld port

Enables or disables UDLD status on a specific port or a range of ports.

udld port *chassis/slot/port***[**-*port2***] {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number.
enable	Enables UDLD status on a port.
disable	Disables UDLD status on a port.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Auto-negotiation should be disabled on both ends of the link for UDLD to operate properly.
- The UDLD protocol must be enabled before using this command.
- The UDLD protocol is supported on link aggregate member ports.

Examples

```
-> udld port 1/1/3 enable
-> udld port 1/1/6-10 enable
-> udld port 1/2/4 disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldPortConfigTable
   alaUdldPortConfigUdldStatus
```

udld mode

Configures the UDLD operational mode on a specific port, a range of ports, or all ports.

udld [port [*chassis/slot/port***[-***port2***]] mode {normal | aggressive}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number.
normal	Specifies UDLD operation in the normal mode.
aggressive	Specifies UDLD operation in the aggressive mode.

Defaults

parameter	default
normal | aggressive	**normal**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The UDLD protocol must be enabled before using this command.
- In case of faulty cable connection, the port which is configured in normal mode of operation is considered to be in the shutdown state.

Examples

```
-> udld mode aggressive
-> udld mode normal
-> udld port 1/1/3 mode aggressive
-> udld port 1/2/4 mode normal
-> udld port 1/2/9-18 mode aggressive
```

Release History

Release 7.1.1; command introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldPortConfigTable
   alaUdldPortConfigUdldMode
```

udld probe-timer

Configures the probe-message advertisement timer on a specific port, a range of ports, or all ports. Probe messages are transmitted periodically after this timer expires.

udld [port [*chassis/slot/port***[-***port2***]] probe-timer** *seconds*

no udld [port [*chassis/slot/port***[-***port2***]] probe-timer**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number.
seconds	The probe-message transmission interval, in seconds.

Defaults

parameter	default
seconds	15

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to reset the probe-message timer to the default value. Note that it is not necessary to specify the probe-message interval to reset it.
- The UDLD protocol must be enabled before using this command.
- Configure probe-advertisement timer with values varying in a range of 12-18 seconds for better convergence time and to avoid burst of probe advertisements.

Examples

```
-> udld probe-timer 20
-> udld port 1/1/3 probe-timer 16
-> udld port 1/1/8-21 probe-timer 18
-> no udld probe-timer
-> no udld port 1/1/3 probe-timer
```

Release History

Release 7.1.1; command introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldPortConfigTable
   alaUdldPortConfigUdldProbeIntervalTimer
```

udld echo-wait-timer

Configures the echo based detection timer on a specific port, a range of ports, or all the ports. This is known as link detection period.

udld [port [*chassis/slot/port***[-***port2***]] echo-wait-timer** *seconds*

no udld [port [*chassis/***]***slot/port***[-***port2***]] echo-wait-timer**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number.
seconds	The echo based detection period, in seconds.

Defaults

parameter	default
seconds	8

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to reset the echo based detection timer to the default value. Note that it is not necessary to specify the echo based timer to reset it.
- The UDLD protocol must be enabled before using this command.
- An echo message is expected in reply from the neighbor within this time duration, otherwise, the port is considered as faulty.

Examples

```
-> udld echo-wait-timer 9
-> udld port 1/1/5 echo-wait-timer 12
-> udld port 1/1/7-16 echo-wait-timer 12
-> no udld echo-wait-timer
-> no udld port 1/1/3 echo-wait-timer
```

Release History

Release 7.1.1; command introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldPortConfigTable
   alaUdldPortConfigUdldDetectionPeriodTimer
```

clear udld statistics port

Clears the UDLD statistics for a specific port or for all the ports.

clear udld statistics [port *chassis/slot/port***]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

If the slot/port option is not specified, UDLD statistics for the switch is cleared.

Examples

```
-> clear udld statistics port 1/1/4
-> clear udld statistics
```

Release History

Release 7.1.1; command introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld statistics port	Displays the UDLD statistics for a specific port.

MIB Objects

```
alaUdldGlobalClearStats
```

show udld configuration

Displays the global status of UDLD configuration.

show udld configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show udld configuration

Global UDLD Status                : disabled,
Global UDLD Mode                  : normal,
Global UDLD Probe Timer (Sec)     : 15,
Global UDLD Echo-Wait Timer (Sec) : 8
Global UDLD Status : Disabled
```

output definitions

Global UDLD Status	Indicates the UDLD status on the switch. Options include **enabled** or **disabled**.
Global UDLD Mode	Indicates the UDLD mode on the switch. Options include **normal** or **aggressive**.
Global UDLD Probe Timer (Sec)	A probe-message is expected after this time period.
Global UDLD Echo-Wait Timer (Sec)	The detection of neighbor is expected with in this time period.
Global UDLD Status	Indicates the UDLD status on the switch. Options include **enabled** or **disabled**.

Release History

Release 7.1.1; command introduced.

Related Commands

udld	Globally enables or disables UDLD protocol on the switch.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldGlobalStatus
   alaUdldGlobalConfigUdldStatus
```

show udld configuration port

Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

show udld configuration port [*chassis/slot/port***]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number.

Defaults

By default, a list of all UDLD ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show udld configuration port

Slot/Port    Admin State    Oper Mode    Probe-Timer    Echo-Wait-Timer
-----------+---------------+------------+-------------+----------------
1/1/1           disabled       normal          15           10
1/1/2           disabled       normal          45           10
1/1/17          disabled       normal          33            8
1/1/18          disabled       normal          33            8
1/1/19          disabled       normal          33            8
1/1/20          disabled       aggresive       55            8
1/1/21          disabled       aggresive       55            8
1/1/22          disabled       aggresive       55            8
1/1/41          disabled       aggresive       77            8
1/1/42          enabled        aggresive       77            8
1/1/43          enabled        aggresive       77            8
1/1/44          enabled        aggresive       77            8
1/1/45          enabled        aggresive       77            8

 -> show udld configuration port 1/1/1

Global UDLD Status           : enabled,
Port UDLD Status             : enabled,
Port UDLD State              : bidirectional,
UDLD Op-Mode                 : aggresive,
Probe Timer (Sec)            : 77,
Echo-Wait Timer (sec)        : 8
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
UDLD-State	Indicates the state of interface determined by UDLD operation, which can be **notapplicable, shutdown, undetermined** or **bidirectional**.
Oper-Mode	Indicates the operational mode of UDLD protocol. Options include **normal** or **aggressive**.
Global UDLD Status	Indicates the UDLD status on the switch. Options include **enabled** or **disabled**.
Port UDLD Status	Indicates the UDLD status on a port. Options include **enable** or **disable**.
Probe Timer	A probe-message is expected after this time period.
Echo-Wait Timer	The detection of neighbor is expected with in this time period.

Release History

Release 7.1.1; command introduced.

Related Commands

udld mode	Configures the operational mode of UDLD on a specific port, a range of ports, or all the ports.
udld probe-timer	Configures the probe-message advertisement timer on a specific port, a range of ports, or all the ports.
udld echo-wait-timer	Configures the echo based detection timer on a specific port, a range of ports, or all the ports.

MIB Objects

```
alaUdldGlobalStatus
   alaUdldGlobalConfigUdldStatus
alaUdldPortConfigTable
   alaUdldPortConfigUdldOperationalStatus
   alaUdldPortConfigUdldMode
   alaUdldPortConfigUdldStatus
   alaUdldPortConfigUdldProbeintervalTimer
   alaUdldPortConfigUdldDetectionPeriodTimer
alaUdldPortNeighborStatsTable
   alaUdldNeighborName
```

show udld statistics port

Displays the UDLD statistics for a specific port.

show udld statistics port *chassis/slot/port*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show udld statistics port 1/1/42

UDLD Port Statistics
 Hello Packet Send        :8,
 Echo Packet Send         :8,
 Flush Packet Recvd       :0
UDLD Neighbor Statistics
 Neighbor ID    Hello Pkts Recv       Echo Pkts Recv
--------------+-------------------+--------------
      1              8              15
      2              8              15
      3              8              21
      4              8              14
      5              8              15
      6              8              20
```

output definitions

Hello Packet Send	The number of hello messages sent by a port.
Echo Packet Send	The number of echo messages sent by a port.
Flush Packet Recvd	The number of UDLD-Flush message received by a port.
Neighbor ID	The name of the neighbor.
Hello Pkts Recv	The number of hello messages received from the neighbor.
Echo Pkts Recv	The number of echo messages received from the neighbor.

Release History

Release 7.1.1; command introduced.

Related Commands

udld probe-timer	Configures the probe-message advertisement timer on a specific port, a range of ports, or all the ports.
udld echo-wait-timer	Configures the echo based detection timer on a specific port, a range of ports, or all the ports.

MIB Objects

```
alaUdldPortNeighborStatsTable
   alaUdldNeighborName
   alaUdldNumHelloSent
   alaUdldNumHelloRcvd
   alaUdldNumEchoSent
   alaUdldNumEchoRcvd
   alaUdldNumFlushRcvd
```

show udld neighbor port

Displays the UDLD neighbor ports.

show udld neighbor port *chassis/slot/port*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show udld neighbor port 1/1/42

 Neighbor ID           Device Id             Port Id
-----------------+--------------------+---------------
      1            00:d0:95:ea:b2:48         00:d0:95:ea:b2:78
      2            00:d0:95:ea:b2:48         00:d0:95:ea:b2:79
      3            00:d0:95:ea:b2:48         00:d0:95:ea:b2:74
      4            00:d0:95:ea:b2:48         00:d0:95:ea:b2:75
      5            00:d0:95:ea:b2:48         00:d0:95:ea:b2:76
      6            00:d0:95:ea:b2:48         00:d0:95:ea:b2:77
```

output definitions

Neighbor ID	The name of the neighbor.
Device ID	The device ID.
Port ID	The port ID.

Release History

Release 7.1.1; command introduced.

Related Commands

udld echo-wait-timer	Configures the echo based detection timer on a specific port, a range of ports, or all the ports. This is known as link detection period.
show udld statistics port	Displays the UDLD statistics for a specific port.

MIB Objects

```
alaUdldPortNeighborStatsTable
   alaUdldNeighborName
```

show udld status port

Displays the UDLD status for all ports or for a specific port.

show udld status port [*chassis/slot/port***]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number.

Defaults

By default, a list of all UDLD ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show udld status port
  Slot/Port        Admin State        Operational State
--------------+------------------+------------------------
    1/1/1             disabled           not applicable
    1/1/2             disabled           not applicable
    1/1/3             disabled           not applicable
    1/1/21            disabled           not applicable
    1/1/40            disabled           not applicable
    1/1/41            disabled           not applicable
    1/1/42            enabled            bidirectional
    1/1/43            enabled            bidirectional
    1/1/44            enabled            bidirectional
    1/1/45            enabled            bidirectional
    1/1/46            enabled            bidirectional
    1/1/47            enabled            bidirectional
    1/1/48            enabled            bidirectional

-> show udld status port 1/1/44
Admin State              : enabled,
Operational State        : bidirectional
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
Admin State	Indicates whether UDLD is administratively **enabled** or **disabled**.
Operational State	Indicates the state of interface determined by UDLD operation, which can be **notapplicable, shutdown, undetermined** or **bidirectional**.

Release History

Release 7.1.1; command introduced.

Related Commands

udld port	Enables or disables UDLD status on a specific port or a range of ports.
show udld configuration port	Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

```
alaUdldGlobalStatus
alaUdldPortConfigTable
   alaUdldPortConfigUdldOperationalStatus
```

4 Source Learning Commands

The Source Learning capability of OmniSwitch is responsible for creating, updating, and deleting source and destination MAC Address entries in the MAC Address Table. This chapter includes descriptions of Source Learning commands used to create or delete static MAC addresses, define the aging time value for static and dynamically learned MAC addresses, and display MAC Address Table entries and statistics.

MIB information for Source Learning commands is as follows:

Filename: ALCATEL-IND1-MAC-ADDRESS-MIB.mib
Module: alcatelIND1MacAddressMIB

A summary of the available commands is listed here:

mac-learning

Configures the status of source MAC address learning on a VLAN, a single port, a range of ports, or on a link aggregate of ports.

mac-learning {vlan *vlan***[-***vlan2***] | port** *chassis/slot/port***[-***port2***] | linkagg** *agg_id***} {enable | disable}**

Syntax Definitions

*vlan***[-***vlan2***]**	The VLAN ID number. Use a hyphen to specify a range of VLAN IDs.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id	The link aggregate ID number.
enable	Enables source learning.
disable	Disables source learning.

Defaults

By default, source learning is enabled on all ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Configuring source learning is not supported on Learned Port Security (LPS) and Universal Network Profile (UNP) ports, as well as individual ports that are members of a link aggregate.
- When port-based source learning is configured for a link aggregate ID, it affects all the ports that are members of the link aggregate.
- When source learning is disabled on a port or link aggregate, dynamic learning of MAC addresses is stopped.
- Static MAC addresses associated with a port or link aggregate are *not* cleared when source learning is disabled. Also, new static MAC address configurations are allowed on ports or link aggregates on which source learning is disabled.
- Disabling source learning on a port or link aggregate is useful on a ring configuration, where switch A does not have to learn MAC addresses from switch B, or for a Transparent LAN Service, where service provider does not require the MAC addresses of the customer network.
- Disabling source learning on a port or link aggregate is not supported on the OmniSwitch 9900.

Examples

```
-> mac-learning port 1/2 enable
-> mac-learning linkagg 10 disable
-> mac-learning vlan 10 disable
```

Release History

Release 7.1.1; command added.

Related Commands

show mac-learning learning-state	Displays the source learning status of a port or link aggregate on the switch.

MIB Objects

```
slMacLearningVlanControlTable
   slMacLearningVlanControlStatus
slMacLearningControlTable
   slMacLearningControlStatus
```

mac-learning flush

Clears the specified MAC addresses from the Source Learning MAC Address Table on the local switch.

mac-learning flush {dynamic | static | multicast} [mac-address *mac_address***]**

Syntax Definitions

dynamic	Clears dynamically learned MAC addresses.
static	Removes static MAC addresses.
multicast	Removes static multicast MAC addresses.
mac_address	Enter the MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c).

Defaults

parameter	default
mac-address	all MAC addresses

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table.
- Static unicast and static multicast addresses are removed. This command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush dynamic
-> mac-learning flush dynamic mac-address 00:00:39:59:f1:0c
-> mac-learning flush static
-> mac-learning flush static mac-address 00:00:39:59:f1:0d
-> mac-learning flush multicast
-> mac-learning flush multicast mac-address 01:25:9a:5c:2f:10
```

Release History

Release 7.3.1; command added.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information for the local switch.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slMacAddressGblRowStatus
```

mac-learning flush domain all

Clears the specified MAC addresses from the Source Learning MAC Address Table for all learning domains on the local switch.

mac-learning flush domain all {dynamic | static}

Syntax Definitions

dynamic	Clears dynamically learned MAC addresses from all of the domains.
static	Removes static MAC addresses from all of the domains.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for all domains.
- Static unicast and static multicast addresses are removed.
- The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush domain all dynamic
-> mac-learning flush domain all static
```

Release History

Release 7.3.1; command added.

Related Commands

mac-learning flush	Clears the MAC Address Table for the local switch.
mac-learning flush domain vlan	Clears MAC addresses from the VLAN learning domain.
mac-learning flush domain spb	Clears MAC addresses from the SPB learning domain.
mac-learning flush domain vxlan	Clears MAC addresses from the VXLAN learning domain.
mac-learning flush domain l2gre	Clears MAC addresses from the L2 GRE tunnel learning domain.
show mac-learning	Displays Source Learning MAC Address Table information for the local switch.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slMacAddressGblRowStatus
```

mac-learning flush domain vlan

Clears the specified MAC addresses from the Source Learning MAC Address Table for the VLAN learning domain on the local switch.

mac-learning flush domain vlan {vlan *vlan_id***} {port** *chassis/slot/port* **| linkagg** *agg_id***} | {dynamic | static | static-multicast} [mac-address** *mac_address***]**

Syntax Definitions

vlan_id	VLAN ID number.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
agg_id	Enter a link aggregate ID number.
dynamic	Clears dynamically learned MAC addresses from the VLAN domain.
static	Removes static MAC addresses from the VLAN domain.
static-multicast	Removes static multicast MAC addresses from the VLAN domain.
mac_address	Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

Defaults

parameter	default
mac-address	all MAC addresses

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the VLAN domain.
- Static unicast and static multicast addresses are removed.
- The **static-multicast** parameter is *not* available for use with the following **mac-learning flush** commands:
  - **mac-learning flush domain all**
  - **mac-learning flush domain spb**
  - **mac-learning flush domain vxlan**
  - **mac-learning flush domain l2gre**
  - **mac-learning flush domain local**
- The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush domain vlan vlan 20 port 1/2 dynamic
-> mac-learning flush domain vlan static
-> mac-learning flush domain vlan linkagg 10 static
```

Release History

Release 7.3.1; command added.

Related Commands

mac-learning flush	Clears the MAC Address Table for the local switch.
mac-learning flush domain spb	Clears MAC addresses from the SPB learning domain.
mac-learning flush domain vxlan	Clears MAC addresses from the VXLAN learning domain.
mac-learning flush domain l2gre	Clears MAC addresses from the L2 GRE tunnel learning domain.
show mac-learning	Displays Source Learning MAC Address Table information for the local switch.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slMacAddressGblRowStatus
```

mac-learning flush domain spb

Clears the specified MAC addresses from the Source Learning MAC Address Table for the Shortest Path Bridging (SPB) learning domain on the local switch.

mac-learning flush domain spb {serviceid *service_id* **| sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id*[:*service_id*] **| isid** *instance_id***} {dynamic | static} [mac-address** *mac_address***]**

Syntax Definitions

service_id	An existing SPB service ID.
chassis	The chassis identifier.
slot/port:encap	The SPB access port and encapsulation (**0**, **all**, *qtag*, or *outer_qtag.inner_qtag*) for an SPB Service Access Point (SAP).
sdp_id[:*service_id*]	Clears MAC addresses learned on an SPB Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are cleared.
instance_id	An SPB backbone service instance identifier (I-SID).
dynamic	Clears dynamically learned MAC addresses from the SPB domain.
static	Removes static MAC addresses from the SPB domain.
mac_address	Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

Defaults

parameter	default
mac-address	all MAC addresses

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the SPB domain.
- Static unicast and static multicast addresses are removed.
- The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush domain spb dynamic
-> mac-learning flush domain spb sap 1/12:0 dynamic
-> mac-learning flush domain spb serviceid 10 isid 1500 dynamic
```

Release History

Release 7.3.1; command added.

Related Commands

mac-learning flush	Clears the MAC Address Table for the local switch.
mac-learning flush domain vlan	Clears MAC addresses from the VLAN learning domain.
mac-learning flush domain vxlan	Clears MAC addresses from the VXLAN learning domain.
mac-learning flush domain l2gre	Clears MAC addresses from the L2 GRE tunnel learning domain.
show mac-learning	Displays Source Learning MAC Address Table information for the local switch.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slSvcISID
   slMacAddressGblRowStatus
```

mac-learning flush domain vxlan

Clears the specified MAC addresses from the Source Learning MAC Address Table for the Virtual eXtensible LAN (VXLAN) learning domain on the local switch.

mac-learning flush domain vxlan {serviceid *service_id* **| sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id*[:*service_id*] **| vnid** *vxlan_id***} {dynamic | static} [mac-address** *mac_address***]**

Syntax Definitions

service_id	An existing VXLAN service ID.
chassis	The chassis identifier.
slot/port:encap	The VXLAN access port and encapsulation (**0**, **all**, *qtag*, or *outer_qtag.inner_qtag*) for a VXLAN Service Access Point (SAP).
sdp_id[:*service_id*]	Clears MAC addresses learned on a VXLAN Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
vxlan_id	A 24-bit numerical value that identifies a VXLAN segment (a VXLAN network ID). The valid range is 1– 2147483647 (or 000.000.001–255.255.255 in decimal notation format). Use a hyphen to specify a range of IDs (25001-25005).
dynamic	Clears dynamically learned MAC addresses from the VXLAN domain.
static	Removes static MAC addresses from the VXLAN domain.
mac_address	Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

Defaults

parameter	default
mac-address	all MAC addresses

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the VXLAN domain.
- Static unicast and static multicast addresses are removed.
- The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush domain vxlan dynamic
-> mac-learning flush domain vxlan sap 1/12:0 dynamic
-> mac-learning flush domain vxlan serviceid 10 vnid 23000 dynamic
```

Release History

Release 7.3.1; command added.

Related Commands

mac-learning flush	Clears the MAC Address Table for the local switch.
mac-learning flush domain vlan	Clears MAC addresses from the VLAN learning domain.
mac-learning flush domain spb	Clears MAC addresses from the SPB learning domain.
mac-learning flush domain l2gre	Clears MAC addresses from the L2 GRE tunnel learning domain.
show mac-learning	Displays Source Learning MAC Address Table information for the local switch.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slVxLanVnID
   slMacAddressGblRowStatus
```

mac-learning flush domain l2gre

Clears the specified MAC addresses from the Source Learning MAC Address Table for the Layer 2 Generic Routing Encapsulation (L2 GRE) learning domain on the local switch.

mac-learning flush domain l2gre {serviceid *service_id* **| sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id*[:*service_id*] **| vpnid** *vpn_id***} {dynamic | static} [mac-address** *mac_address***]**

Syntax Definitions

service_id	An existing L2 GRE service ID.
chassis	The chassis identifier.
slot/port:encap	The access port and encapsulation (**0**, **all**, *qtag*, or *outer_qtag.inner_qtag*) for an L2 GRE Service Access Point (SAP).
sdp_id[:*service_id*]	Clears MAC addresses learned on an L2 GRE Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
vpn_id	A tunnel ID that identifies a GRE tunnel VPN.
dynamic	Clears dynamically learned MAC addresses from the L2 GRE domain.
static	Removes static MAC addresses from the L2 GRE domain.
mac_address	Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

Defaults

parameter	default
mac-address	all MAC addresses

Platforms Supported

OmniSwitch 6860, 6865, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the L2 GRE tunnel domain.
- Static unicast and static multicast addresses are removed.
- The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush domain l2gre dynamic
-> mac-learning flush domain l2gre sap 1/1/12:0 dynamic
-> mac-learning flush domain l2gre serviceid 10 vpnid 200 dynamic
```

Release History

Release 8.4.1.R02; command introduced.

Related Commands

mac-learning flush	Clears the MAC Address Table for the local switch.
mac-learning flush domain vlan	Clears MAC addresses from the VLAN learning domain.
mac-learning flush domain spb	Clears MAC addresses from the SPB learning domain.
mac-learning flush domain vxlan	Clears MAC addresses from the VXLAN learning domain.
show mac-learning	Displays Source Learning MAC Address Table information for the local switch.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slL2GreVpnID
   slMacAddressGblRowStatus
```

mac-learning flush domain local

Clears the specified MAC addresses from the Source Learning MAC address table for the local service learning domain.

mac-learning flush domain local serviceid *service_id* **[sap** *chassis/slot/port:encap***] static [mac-address** *mac_address***]**

Syntax Definitions

service_id	An existing service ID.
chassis	The chassis identifier.
slot/port:encap	The service access port and encapsulation (**0**, **all**, *qtag*, or *outer_qtag.inner_qtag*) for a Service Access Point (SAP).
mac_address	Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).

Defaults

parameter	default
mac-address	all MAC addresses

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the service domain.
- Static unicast and static multicast addresses are removed.
- The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush domain local serviceid 10 static
-> mac-learning flush domain local serviceid 20 sap 1/1/13:20 static
```

Release History

Release 7.3.1; command added.

Related Commands

mac-learning flush	Clears the MAC Address Table for the local switch.
mac-learning flush domain vlan	Clears MAC addresses from the VLAN learning domain.
mac-learning flush domain spb	Clears MAC addresses from the Shortest Path Bridging (SPB) learning domain.
mac-learning flush domain vxlan	Clears MAC addresses from the Virtual eXtensible LAN (VXLAN) learning domain.
show mac-learning	Displays Source Learning MAC address table information for the local switch.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblProtocol
   slMacAddressGblGroupField
```

mac-learning static mac-address

Configures a static destination unicast MAC address. The configured MAC address is assigned to a fixed switch port or link aggregate ID and VLAN. If the destination of the data packets received on the VLAN ports is the configured MAC address, then they are forwarded to the specific MAC address port.

mac-learning {vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}} static mac-address** *mac_address* **[bridging | filtering]**

mac-learning flush [vlan *vlan_id* **[port** *chassis/slot/port* | **linkagg** *agg_id***]] static [mac-address** *mac_address***]**

Syntax Definitions

vlan_id	VLAN ID number.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1) that is assigned to the static MAC address.
agg_id	Enter a link aggregate ID number. See Chapter 12, "Link Aggregation Commands."
mac_address	Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
bridging	Specifies that all packets to or from this MAC address are bridged.
filtering	Specifies that all packets to or from this MAC address are filtered or dropped.

Defaults

parameter	default
bridging | filtering	bridging

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **mac-learning flush** command to remove a static MAC address from the Source Learning MAC Address Table. Note that If no parameters are specified with this command, then all static addresses are removed.
- Enter a port number or link aggregate ID that is already associated with the specified VLAN ID. Only traffic from other ports associated with the same VLAN is directed to the static MAC address port.
- Select the **filtering** parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the **bridging** parameter for regular traffic flow to or from the MAC address.
- The destination MAC addresses are maintained in the Source Learning MAC address table.

- If a packet received on a port associated with the same VLAN contains a source address that matches a static MAC address, then the packet is discarded.

Examples

```
-> mac-learning vlan 10 port 1/10 static mac-address 00:00:39:59:f1:0c bridging
-> mac-learning vlan 20 linkagg 5 static mac-address 00:00:9a:55:e0:01 filtering
-> mac-learning flush vlan 500 static
-> mac-learning flush vlan 10 port 1/10 static mac-address 00:00:39:59:f1:0c
-> mac-learning flush vlan 20 linkagg 5 static
-> mac-learning flush static
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1: **mac-learning flush** command replaced the **no mac-learning** command.

Related Commands

vlan members untagged	Assigns ports and link aggregates to a VLAN.
mac-learning multicast mac-address	Configures a static multicast MAC address and assigns the address to one or more egress ports or link aggregates.
show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
alaSlMacAddressGlobalTable
   slOriginId
   slServiceId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
```

mac-learning domain vlan static mac-address

Configures a static destination unicast MAC address in the VLAN source learning domain. The configured MAC address is assigned to a fixed switch port or link aggregate ID and VLAN. If the destination of the data packets received on the VLAN ports is the configured static MAC address, then they are forwarded to the specific MAC address port.

mac-learning domain vlan vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***} static mac-address** *mac_address* **[bridging | filtering]**

mac-learning flush domain vlan [vlan *vlan_id* **[port** *chassis/slot/port* | **linkagg** *agg_id***]] static [mac-address** *mac_address***]**

Syntax Definitions

vlan_id	VLAN ID number.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1) that is assigned to the static MAC address.
agg_id	Enter a link aggregate ID number. See Chapter 12, "Link Aggregation Commands."
mac_address	Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
bridging	Specifies that all packets to or from this MAC address are bridged.
filtering	Specifies that all packets to or from this MAC address are filtered or dropped.

Defaults

parameter	default
bridging | filtering	bridging

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **mac-learning flush** command to remove a static MAC address from the Source Learning MAC Address Table. Note that If no parameters are specified with this command, then all static addresses are removed.
- Enter a port number or link aggregate ID that is already associated with the specified VLAN ID. Only traffic from other ports associated with the same VLAN is directed to the static MAC address port.
- Select the **filtering** parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the **bridging** parameter for regular traffic flow to or from the MAC address.
- The destination MAC addresses are maintained in the Source Learning MAC address table.

- If a packet received on a port associated with the same VLAN contains a source address that matches a static MAC address, then the packet is discarded.

Examples

```
-> mac-learning domain vlan vlan 10 port 1/1/10 static mac-address
00:00:39:59:f1:0c bridging
-> mac-learning domain vlan vlan 20 linkagg 5 static mac-address 00:00:9a:55:e0:01
filtering
-> mac-learning flush domain vlan vlan 500 static
-> mac-learning flush domain vlan vlan 10 port 1/1/10 static mac-address
00:00:39:59:f1:0c
-> mac-learning flush domain vlan vlan 20 linkagg 5 static
-> mac-learning flush domain vlan static
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1: **mac-learning flush** command replaced the **no mac-learning** command.

Related Commands

vlan members untagged	Assigns ports and link aggregates to a VLAN.
mac-learning flush domain vlan	Clears MAC addresses from the VLAN source learning domain.
show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slOriginId
   slServiceId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
```

mac-learning domain spb static mac-address

Configures a static destination unicast MAC address in the Shortest Path Bridging (SPB) source learning domain.

mac-learning domain spb {serviceid *service_id* **{isid** *instance_id* **| sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id*:*service_id***} static mac-address** *mac_address* **[bridging | filtering]**

mac-learning domain spb {isid *instance_id* **{sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id*:*service_id***} static mac-address** *mac_address* **[bridging | filtering]**

mac-learning flush domain spb {serviceid *service_id* **| sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id*[:*service_id*] **| isid** *instance_id***} static [mac-address** *mac_address***]**

Syntax Definitions

service_id	An existing SPB service ID.
instance_id	An SPB backbone service instance identifier (I-SID).
chassis	The chassis identifier.
slot/port:encap	The SPB access port and encapsulation (**0**, *qtag*, or *outer_qtag.inner_qtag*) for an SPB Service Access Point (SAP).
sdp_id:*service_id*	The SPB Service Distribution Point (SDP) ID number and service ID number for a specific binding.
mac_address	Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
bridging	Specifies that all packets to or from this MAC address are bridged.
filtering	Specifies that all packets to or from this MAC address are filtered or dropped.

Defaults

parameter	default
bridging | filtering	bridging

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **mac-learning flush** command to remove a static MAC address from the Source Learning MAC Address Table. Note that If no parameters are specified with this command, then all static addresses are removed.
- Select the **filtering** parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the **bridging** parameter for regular traffic flow to or from the MAC address.
- The destination MAC addresses are maintained in the Source Learning MAC address table.

- If a packet received on an access port associated with the same SAP contains a source address that matches a static MAC address, then the packet is discarded.

Examples

```
-> mac-learning domain spb serviceid 10 sap 1/1/12:0 static mac-address
00:00:39:59:f1:0c bridging
-> mac-learning domain spb isid 1500 sap 1/1/12:0 static mac-address
00:00:39:59:f1:0c filtering
-> mac-learning flush domain spb static
-> mac-learning flush domain spb sap 1/1/12:0 static mac-address 00:00:39:59:f1:0c
-> mac-learning flush domain spb serviceid 10 isid 1500 static
```

Release History

Release 7.3.1; command added.

Related Commands

mac-learning flush domain spb	Clears MAC addresses from the SPB source learning domain.
mac-learning domain vlan static mac-address	Configures static MAC addresses in the VLAN source learning domain.
mac-learning domain vxlan static mac-address	Configures static MAC addresses in the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning domain spb	Displays MAC Address Table information for the SPB source learning domain.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblProtocol
   slMacAddressGblGroupField
   slSvcISID
```

mac-learning domain vxlan static mac-address

Configures a static destination unicast MAC address in the Virtual eXtensible LAN (VXLAN) source learning domain

mac-learning domain vxlan {serviceid *service_id* **{sap** *chassis/slot/port:encap* **| vnid** *vxlan_id* **[sap** *chassis/slot/port:encap***]} static mac-address** *mac_address* **[bridging | filtering]**

mac-learning domain vxlan vnid *vxlan_id* **sap** *chassis/slot/port:encap* **static mac-address** *mac_address* **[bridging | filtering]**

mac-learning flush domain vxlan {serviceid *service_id* **| sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id*[:*service_id*] **| vnid** *vxlan_id***} static [mac-address** *mac_address***]**

Syntax Definitions

service_id	An existing VXLAN service ID.
chassis	The chassis identifier.
slot/port:encap	The VXLAN access port and encapsulation (*qtag*, or *outer_qtag.inner_qtag*) for a VXLAN Service Access Point (SAP).
vxlan_id	A 24-bit numerical value that identifies an existing VXLAN segment (a VXLAN network ID).
mac_address	Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
bridging	Specifies that all packets to or from this MAC address are bridged.
filtering	Specifies that all packets to or from this MAC address are filtered or dropped.
sdp_id[:*service_id*]	Use this parameter with the **mac-learning flush** command to specify a VXLAN Service Distribution Point (SDP) ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are cleared.

Defaults

parameter	default
bridging | filtering	bridging

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32

Usage Guidelines

- Use the **mac-learning flush** command to remove a static MAC address from the Source Learning MAC address table. Note that If no parameters are specified with this command, then all static addresses are removed.

- Select the **filtering** parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the **bridging** parameter for regular traffic flow to or from the MAC address.
- The destination MAC addresses are maintained in the Source Learning MAC address table.
- If a packet received on an access port associated with the same SAP contains a source address that matches a static MAC address, then the packet is discarded.

Examples

```
-> mac-learning domain vxlan serviceid 10 sap 1/1/12:10 static mac-address
00:00:39:59:f1:0c bridging
-> mac-learning domain vxlan vnid 23000 sap 1/1/12:10 static mac-address
00:00:39:59:f1:0c filtering
-> mac-learning flush domain vxlan static
-> mac-learning flush domain vxlan sap 1/12:0 static
-> mac-learning flush domain vxlan serviceid 10 vnid 23000 static
```

Release History

Release 7.3.1; command added.

Related Commands

mac-learning flush domain vxlan	Clears MAC addresses from the VXLAN source learning domain.
mac-learning domain vlan static mac-address	Configures static MAC addresses in the VLAN source learning domain.
mac-learning domain spb static mac-address	Configures static MAC addresses in the Shortest Path Bridging (SPB) source learning domain.
show mac-learning domain vxlan	Displays MAC Address Table information for the VXLAN source learning domain.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblProtocol
   slMacAddressGblGroupField
   slVxLanVnID
```

mac-learning domain local static mac-address

Configures a static destination unicast MAC address for a local service in the source learning domain

mac-learning domain local serviceid *service_id* **sap** *chassis/slot/port:encap* **static mac-address** *mac_address* **[bridging | filtering]**

mac-learning flush domain local serviceid *service_id* **[sap** *chassis/slot/port:encap***] static [mac-address** *mac_address***]**

Syntax Definitions

service_id	An existing service ID.
chassis	The chassis identifier.
slot/port:encap	The service access port and encapsulation (*qtag*, or *outer_qtag.inner_qtag*) for a VXLAN Service Access Point (SAP).
mac_address	Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
bridging	Specifies that all packets to or from this MAC address are bridged.
filtering	Specifies that all packets to or from this MAC address are filtered or dropped.

Defaults

parameter	default
bridging | filtering	bridging

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **mac-learning flush** command to remove a static MAC address from the Source Learning MAC address table. Note that If no parameters are specified with this command, then all static addresses are removed.
- Select the **filtering** parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the **bridging** parameter for regular traffic flow to or from the MAC address.
- The destination MAC addresses are maintained in the Source Learning MAC address table.
- If a packet received on an access port associated with the same SAP contains a source address that matches a static MAC address, then the packet is discarded.

Examples

```
-> mac-learning domain local serviceid 10 sap 1/1/12:10 static mac-address
00:00:39:59:f1:0c bridging
-> mac-learning domain local serviceid 20 sap 1/1/13:20 static mac-address
00:00:39:59:f1:0c filtering
-> mac-learning flush domain local serviceid 10 static
-> mac-learning flush domain local serviceid 20 sap 1/1/13:20 static
```

Release History

Release 7.3.1; command added.

Related Commands

mac-learning flush domain vxlan	Clears MAC addresses from the VXLAN source learning domain.
mac-learning domain vlan static mac-address	Configures static MAC addresses in the VLAN source learning domain.
mac-learning domain spb static mac-address	Configures static MAC addresses in the Shortest Path Bridging (SPB) source learning domain.
mac-learning domain vxlan static mac-address	Configures static MAC addresses in the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning domain local	Displays MAC Address Table information for the Local source learning domain.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblProtocol
   slMacAddressGblGroupField
```

mac-learning multicast mac-address

Configures a static multicast MAC address and assigns the address to one or more egress ports. Packets received on ports associated with the specified VLAN that contain a destination MAC address that matches the static multicast address are forwarded to the specified egress ports. Static multicast MAC addresses are maintained in the Source Learning MAC address table.

mac-learning {vlan *vlan_id* **{port** *chassis/slot/port* **| linkagg** *agg_id* **}} multicast mac-address** *multicast_address* **[group** *group_id***]**

mac-learning flush [vlan *vlan_id* **[port** *chassis/slot/port* **| linkagg** *agg_id* **]] multicast [mac-address** *multicast_address***]**

Syntax Definitions

vlan_id	VLAN ID number.
chassis	The chassis identifier.
slot/port	The egress slot and port number (3/1) that is assigned to the static multicast MAC address.
agg_id	Enter a link aggregate ID number. See Chapter 12, "Link Aggregation Commands."
multicast_address	Enter the destination multicast MAC Address to add to the MAC Address Table (for example, 01:00:39:59:f1:0c).
group_id	*This keyword cannot be user defined.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **mac-learning flush** command to remove a static multicast MAC address from the Source Learning MAC Address Table. Note that If no parameters are specified with this command, then all static multicast addresses are removed.
- Note that a MAC address is considered a multicast MAC address if the least significant bit of the most significant octet of the address is enabled. For example, MAC addresses with a prefix of 01, 03, 05, 13, and so on, are multicast MAC addresses.
- If a multicast prefix value is not present, then the address is treated as a regular MAC address and not allowed when using the **mac-learning vlan multicast mac-address** command. Also note that multicast addresses within the following ranges are not supported:

  01:00:5E:00:00:00 to 01:00:5E:7F:FF:FF
  01:80:C2:XX.XX.XX
  33:33:XX:XX:XX:XX

- The configured (static) multicast MAC address is assigned to a fixed switch port or link aggregate ID and VLAN.
- In addition to configuring the same static multicast address for multiple ports within a given VLAN, it is also possible to use the same multicast address across multiple VLANs.
- Enter a port number or link aggregate ID that is already associated with the specified VLAN ID. Only traffic from other ports associated with the same VLAN is directed to the static MAC address port.
- If the **configuration snapshot** or **write memory** command is entered after a static multicast MAC address is configured, the resulting ASCII file or **boot.cfg** file includes the "**group** *group_id*" as the additional syntax for the **mac-learning static-multicast** command. The "**group** *group_id*" indicates the number of the multicast group that the switch has assigned to the multicast MAC address for the given VLAN association. Each multicast address – VLAN association is treated as a unique instance and assigned a group number specific to that instance.
- Note that if the port assigned to a multicast MAC address is down or administratively disabled when the **configuration snapshot** or **write memory** command is used, the multicast MAC address is not saved to the resulting ASCII file or **boot.cfg** file.

Examples

```
-> mac-learning vlan 1500 port 1/10 multicast mac-address 01:25:9a:5c:2f:10
-> mac-learning vlan 355 port 4/2-10 multicast mac-address 01:25:9a:5c:2f:11
-> mac-learning vlan 455 linkagg 10 multicast mac-address 01:25:9a:5c:2f:12
-> mac-learning flush vlan 500 multicast
-> mac-learning flush vlan 1500 port 1/10 multicast mac-address 01:25:9a:5c:2f:10
-> mac-learning flush vlan 455 linkagg 10 multicast mac-address 01:25:9a:5c:2f:12
-> mac-learning flush multicast
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; **mac-learning flush** command replaced the **no mac-learning command**.

Related Commands

vlan members untagged	Assigns ports and link aggregates to a VLAN.
mac-learning static mac-address	Configures a static MAC address and assigns the address to a port or link aggregate.
show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
alaSlMacAddressGlobalTable
   slOriginId
   slServiceId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
```

mac-learning aging-time

Configures aging time, in seconds, for static and dynamically learned MAC addresses. When a MAC address has aged beyond the aging-time value, the MAC address is discarded.

mac-learning aging-time {*seconds* **| default}**

no mac-learning aging-time

Syntax Definitions

seconds	Aging time value (in seconds). Do not use commas in value.
default	The aging time is set to the default value of 300 seconds.

Defaults

By default, the aging time is set to 300 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **default** parameter to set the aging-time back to the default value of 300 seconds.
- The aging time value is a global value that applies to all VLANs. Configuring this value on a per VLAN basis is not supported.
- Note that an inactive MAC address can take up to twice as long as the aging time value specified to be removed from the MAC address table. For example, if an aging time of 60 seconds is specified, the MAC address ages out any time between 60 and 120 seconds of inactivity.
- When a new MAC aging time is set, the aging process could take up to 3 aging cycles to age out the inactive macs. This only applies to the first time the aging time is set. Subsequent aging processes can take up to twice as long as the aging time value as described above.
- The MAC address table aging time is also used as the timeout value for the Address Resolution Protocol (ARP) table. This timeout value determines how long the switch retains dynamically learned ARP table entries.

Examples

```
-> mac-learning aging-time 1200
-> mac-learning aging-time default
```

Release History

Release 7.1.1; command introduced.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
slMacAddressAgingTable
   slMacAgingValue
```

mac-learning mode

Specifies the source learning mode for the chassis.

mac-learning mode [centralized | distributed]

Syntax Definitions

centralized	Enables centralized MAC source learning mode.
distributed	Enables distributed MAC source learning mode.

Defaults

By default, centralized MAC source learning mode is enabled for the chassis.

Platforms Supported

Not supported in this release.

Usage Guidelines

After the distributed MAC mode is either enabled or disabled using this command, immediately save the switch configuration using the **write memory** command and then reboot the switch.

Examples

```
-> mac-learning mode centralized
-> mac-learning mode distributed
```

Release History

Release 7.1.1; command introduced.

Related Commands

show mac-learning mode	Displays the current status of the MAC source learning mode.

MIB Objects

```
slDistributedMacMode
```

show mac-learning

Displays Source Learning MAC Address Table information for the switch.

show mac-learning [summary | dynamic | static | multicast | bmac] [port *chassis/slot/port***] [linkagg** *agg_id***] [mac-address** *mac_address***] [remote [mac-address** *mac_address***]]**

Syntax Definitions

summary	Displays a summary of all the MAC address information.
dynamic	Displays only dynamically learned MAC addresses.
static	Displays only static MAC addresses with a permanent status.
multicast	Displays only multicast MAC addresses.
bmac	Displays only backbone MAC addresses (BMACs). A BMAC is the bridge MAC address of a Shortest Path Bridging (SPB) switch.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
agg_id	The link aggregate ID number.
mac_address	A MAC Address (for example, 00:00:39:59:f1:0c).

Defaults

By default, information is displayed for all MAC addresses contained in the table.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the **show mac-learning** command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
- If there is a duplicate static MAC address occurence, a “&” will appear to the right of the address in the **show mac-learning** command display.

Examples

```
-> show mac-learning summary
Mac Address Table Summary:

   Domain       Static     Static-Multicast       Bmac        Dynamic
------------+------------+------------------+------------+------------
    VLAN              0                  0           12           12
     SPB              0                  0            0            6
   LOCAL              0                  0            0            0
   VXLAN              0                  0            0            4
   L2GRE              0                  0            0            0

 Total MAC Address In Use  = 34

-> show mac-learning
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+-----------------+--------+----------+--------------
  VLAN                    10  e8:e7:32:11:d4:78  dynamic   bridging          1/1/14
  VLAN                    52  e8:e7:32:42:e0:4d  dynamic   bridging           1/5/3
  VLAN                    60  e8:e7:32:40:10:7e  dynamic   bridging          1/5/14
  VLAN                    60  e8:e7:32:00:24:a5  dynamic   bridging             0/1
  VLAN                    60  e8:e7:32:00:24:b3  dynamic   bridging             0/1
  VLAN                    60  e8:e7:32:6c:5c:de  dynamic   bridging            0/92
  VLAN                   100  e8:e7:32:42:e0:4d  dynamic   bridging            0/98
  VLAN                   108  e8:e7:32:42:d8:6d  dynamic   bridging            0/16
  VLAN                   208  e8:e7:32:42:e0:dd  dynamic   bridging            0/15
  VLAN                  1000  e8:e7:32:00:27:e1  dynamic   bridging          1/1/14
  VLAN                  1000  e8:e7:32:00:27:ee  dynamic   bridging          1/1/14
  VLAN                  1000  e8:e7:32:40:10:7e  dynamic   bridging          1/1/14
  VLAN                  4000  e8:e7:32:00:27:e1     bmac   bridging          1/5/14
  VLAN                  4000  e8:e7:32:40:10:7e     bmac   bridging          1/5/14
  VLAN                  4000  e8:e7:32:00:24:a5     bmac   bridging             0/1
  VLAN                  4000  e8:e7:32:6c:5c:de     bmac   bridging            0/91
  VLAN                  4051  e8:e7:32:00:27:e1     bmac   bridging          1/5/14
  VLAN                  4051  e8:e7:32:40:10:7e     bmac   bridging          1/5/14
  VLAN                  4051  e8:e7:32:00:24:a5     bmac   bridging             0/1
  VLAN                  4051  e8:e7:32:6c:5c:de     bmac   bridging            0/91
  VLAN                  4052  e8:e7:32:00:27:e1     bmac   bridging          1/5/14
  VLAN                  4052  e8:e7:32:40:10:7e     bmac   bridging          1/5/14
  VLAN                  4052  e8:e7:32:00:24:a5     bmac   bridging             0/1
  VLAN                  4052  e8:e7:32:6c:5c:de     bmac   bridging            0/91
   SPB             1000:1000  e8:e7:32:11:db:72  dynamic  servicing sap:1/1/13:1000
   SPB             1000:1000  e8:e7:32:40:10:7e  dynamic  servicing  sdp:32867:1000
   SPB             1000:1000  e8:e7:32:00:27:e1  dynamic  servicing  sdp:32904:1000
   SPB             1000:1000  e8:e7:32:00:27:ee  dynamic  servicing  sdp:32904:1000
   SPB             3899:3899  e8:e7:32:42:e0:4d  dynamic  servicing     sap:0/99:99
   SPB             3899:3899  e8:e7:32:42:e0:5c  dynamic  servicing     sap:0/99:99
 VXLAN                 5:5  00:0e:1e:06:87:8c  dynamic  servicing     sap:1/1/20A
 VXLAN                 5:5  00:c0:dd:10:2c:c1  dynamic  servicing     sap:1/1/20A
 VXLAN                 5:5  00:0e:1e:0c:58:94  dynamic  servicing       sdp:175:5
 VXLAN                 5:5  46:91:54:dc:6e:41  dynamic  servicing       sdp:175:5

Total number of Valid MAC addresses above = 34
```

```
-> show mac-learning bmac
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain  Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
-------+----------------------+----------------+--------+----------+------------
  VLAN                    4000  e8:e7:32:00:27:e1     bmac   bridging        1/5/14
  VLAN                    4000  e8:e7:32:40:10:7e     bmac   bridging        1/5/14
  VLAN                    4000  e8:e7:32:00:24:a5     bmac   bridging           0/1
  VLAN                    4000  e8:e7:32:6c:5c:de     bmac   bridging          0/91
  VLAN                    4051  e8:e7:32:00:27:e1     bmac   bridging        1/5/14
  VLAN                    4051  e8:e7:32:40:10:7e     bmac   bridging        1/5/14
  VLAN                    4051  e8:e7:32:00:24:a5     bmac   bridging           0/1
  VLAN                    4051  e8:e7:32:6c:5c:de     bmac   bridging          0/91
  VLAN                    4052  e8:e7:32:00:27:e1     bmac   bridging        1/5/14
  VLAN                    4052  e8:e7:32:40:10:7e     bmac   bridging        1/5/14
  VLAN                    4052  e8:e7:32:00:24:a5     bmac   bridging           0/1
  VLAN                    4052  e8:e7:32:6c:5c:de     bmac   bridging          0/91

Total number of Valid MAC addresses above = 12
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured (**VLAN**, **SPB, VXLAN, L2GRE**).
Vlan/ServcId/[ISId/vnID]	This field contains one of the following values depending on the domain type associated with the MAC address: • The VLAN ID number. • The SPB or VXLAN service ID number. • The ISID number associated with the SPB service ID number. • The VXLAN Network ID (VNID) number associated with the VXLAN service ID. • The GRE tunnel VPN ID number associated with the L2 GRE tunnel service ID.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static, bmac).**
Operation	The disposition of the MAC address (**bridging**, **filtering**, **servicing**).
Interface	The slot/port number that is associated with the static or dynamically learned MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29). In the service domain, the Service Access Point (SAP) or the Service Distribution Point (SDP) associated with the MAC address is displayed.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain and service information.
Release 7.3.4; **vnID** field added.

Related Commands

show mac-learning domain vlan	Displays MAC Address Table information for the VLAN source learning domain.
show mac-learning domain spb	Displays MAC Address Table information for the Shortest Path Bridging (SPB source learning domain.
show mac-learning domain vxlan	Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning domain l2gre	Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblGroupField
   slSvcISID
   slVxLanVnID
   slL2GreVpnID
```

show mac-learning domain all

Displays MAC Address Table information for all source learning domains.

show mac-learning domain all [summary]

Syntax Definitions

summary	Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

Examples

```
-> show mac-learning domain all summary
Mac Address Table Summary:

   Domain       Static     Static-Multicast       Bmac        Dynamic
-----------+------------+------------------+------------+------------
    VLAN               0                  0            0           12
    VPLS               0                  0            0            0
     SPB               0                  0            0            0
   LOCAL               0                  0            0            0
   VXLAN               0                  0            0            4
   L2GRE               0                  0            0            0

 Total MAC Address In Use  = 16

-> show mac-learning domain all
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
  VLAN                     1  e8:e7:32:e4:0d:95  dynamic   bridging         1/1/29B
  VLAN                     1  e8:e7:32:e4:0d:96  dynamic   bridging         1/1/29C
```

```
 VLAN                  1  e8:e7:32:e4:0d:97  dynamic   bridging          1/1/29D
 VLAN                  1  e8:e7:32:40:0b:9e  dynamic   bridging             0/24
 VLAN                 46  e8:e7:32:36:1e:f6  dynamic   bridging             0/24
 VLAN                 46  e8:e7:32:40:0b:9e  dynamic   bridging             0/24
 VLAN                 71  00:0e:1e:06:87:88  dynamic   bridging          1/1/20B
 VLAN                 71  00:c0:dd:10:2c:c0  dynamic   bridging          1/1/20B
 VLAN               1024  00:e0:b1:e7:17:a5  dynamic   bridging             0/25
 VLAN               1024  e8:e7:32:26:b6:0e  dynamic   bridging             0/25
 VLAN               1026  00:e0:b1:db:c3:f1  dynamic   bridging             0/24
 VLAN               1026  e8:e7:32:40:0b:9e  dynamic   bridging             0/24
VXLAN                5:5  00:0e:1e:06:87:8c  dynamic  servicing     sap:1/1/20A
VXLAN                5:5  00:c0:dd:10:2c:c1  dynamic  servicing     sap:1/1/20A
VXLAN                5:5  00:0e:1e:0c:58:94  dynamic  servicing       sdp:175:5
VXLAN                5:5  46:91:54:dc:6e:41  dynamic  servicing       sdp:175:5

Total number of Valid MAC addresses above = 16
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured (**VLAN**, **SPB, VXLAN, L2GRE**).
Vlan/ServcId/[ISId/vnID]	This field contains one of the following values depending on the domain type associated with the MAC address: • The VLAN ID number. • The SPB or VXLAN service ID number. • The ISID number associated with the SPB service ID number. • The VXLAN Network ID (VNID) number associated with the VXLAN service ID. • The GRE tunnel VPN ID number associated with the L2 GRE tunnel service ID.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static, bmac).**
Operation	The disposition of the MAC address (**bridging**, **filtering**, **servicing**).
Interface	The slot/port number that is associated with the static or dynamically learned MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29). In the service domain, the Service Access Point (SAP) or the Service Distribution Point (SDP) associated with the MAC address is displayed.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain information.
Release 7.3.4; **vnID** field added.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information for the switch.
show mac-learning domain vlan	Displays MAC Address Table information for the VLAN source learning domain.
show mac-learning domain spb	Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.
show mac-learning domain vxlan	Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning domain l2gre	Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slOriginId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblGroupField
```

show mac-learning domain vlan

Displays MAC Address Table information for the VLAN source learning domain.

show mac-learning domain vlan [vlan *vlan_id***] [port** *chassis/slot/port* **| linkagg** *agg_id***] [dynamic | static | static-multicast | bmac] [mac-address** *mac_address***] [summary]**

Syntax Definitions

vlan_id	VLAN ID number.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1) that is assigned to the static MAC address.
agg_id	A link aggregate ID number.
dynamic	Displays dynamically learned MAC addresses.
static	Displays static MAC addresses with a permanent status.
static-multicast	Displays static multicast MAC addresses. This parameter applies only to the VLAN domain.
bmac	Displays backbone MAC addresses (BMACs). A BMAC is the bridge MAC address of a SPB switch. This parameter applies only to the VLAN domain.
mac_address	A MAC Address (for example, 00:00:39:59:f1:0c).
summary	Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned for the VLAN domain are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

Examples

```
-> show mac-learning domain vlan summary
Mac Address Table Summary:

   Domain       Static     Static-Multicast       Bmac        Dynamic
------------+------------+------------------+-----------+------------
    VLAN               0                  0          12           17

Total MAC Address In Use  = 29

-> show mac-learning domain vlan
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
  VLAN                    71  00:0e:1e:06:87:88  dynamic   bridging         1/1/20B
  VLAN                    71  00:c0:dd:10:2c:c0  dynamic   bridging         1/1/20B
  VLAN                     1  e8:e7:32:e4:0d:95  dynamic   bridging         1/1/29B
  VLAN                     1  e8:e7:32:e4:0d:96  dynamic   bridging         1/1/29C
  VLAN                     1  e8:e7:32:e4:0d:97  dynamic   bridging         1/1/29D
  VLAN                     1  00:00:c9:e3:a1:5f  dynamic   bridging            0/24
  VLAN                     1  e8:e7:32:40:0b:9e  dynamic   bridging            0/24
  VLAN                    46  e8:e7:32:36:1e:f6  dynamic   bridging            0/24
  VLAN                    46  e8:e7:32:40:0b:9e  dynamic   bridging            0/24
  VLAN                   312  00:00:5e:00:01:d4  dynamic   bridging            0/24
  VLAN                   312  00:e0:b1:db:c3:f1  dynamic   bridging            0/24
  VLAN                   312  e8:e7:32:26:b6:0e  dynamic   bridging            0/24
  VLAN                   312  e8:e7:32:40:0b:9e  dynamic   bridging            0/24
  VLAN                   313  00:00:5e:00:01:d5  dynamic   bridging            0/24
  VLAN                   313  00:e0:b1:db:c3:f1  dynamic   bridging            0/24
  VLAN                   313  e8:e7:32:26:b6:0e  dynamic   bridging            0/24
  VLAN                   313  e8:e7:32:40:0b:9e  dynamic   bridging            0/24

Total number of Valid MAC addresses above = 17

-> show mac-learning domain vlan vlan 312
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
  VLAN                   312  00:00:5e:00:01:d4  dynamic   bridging            0/24
  VLAN                   312  00:e0:b1:db:c3:f1  dynamic   bridging            0/24
  VLAN                   312  e8:e7:32:26:b6:0e  dynamic   bridging            0/24
  VLAN                   312  e8:e7:32:40:0b:9e  dynamic   bridging            0/24

 Total number of Valid MAC addresses above = 4
```

```
-> show mac-learning domain vlan port 1/1/20
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
  VLAN                    71  00:0e:1e:06:87:88  dynamic   bridging          1/1/20
  VLAN                    71  00:c0:dd:10:2c:c0  dynamic   bridging          1/1/20

Total number of Valid MAC addresses above = 2

-> show mac-learning domain vlan bmac
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
  VLAN                  4000  e8:e7:32:00:27:e1     bmac   bridging          1/5/14
  VLAN                  4000  e8:e7:32:40:10:7e     bmac   bridging          1/5/14
  VLAN                  4000  e8:e7:32:00:24:a5     bmac   bridging             0/1
  VLAN                  4000  e8:e7:32:6c:5c:de     bmac   bridging            0/91
  VLAN                  4051  e8:e7:32:00:27:e1     bmac   bridging          1/5/14
  VLAN                  4051  e8:e7:32:40:10:7e     bmac   bridging          1/5/14
  VLAN                  4051  e8:e7:32:00:24:a5     bmac   bridging             0/1
  VLAN                  4051  e8:e7:32:6c:5c:de     bmac   bridging            0/91
  VLAN                  4052  e8:e7:32:00:27:e1     bmac   bridging          1/5/14
  VLAN                  4052  e8:e7:32:40:10:7e     bmac   bridging          1/5/14
  VLAN                  4052  e8:e7:32:00:24:a5     bmac   bridging             0/1
  VLAN                  4052  e8:e7:32:6c:5c:de     bmac   bridging            0/91

Total number of Valid MAC addresses above = 12
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured.
Vlan/ServcId/[ISId/vnID]	The VLAN ID number associated with the MAC address.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static, bmac).**
Operation	The disposition of the MAC address (**bridging**, **filtering**, **servicing**).
Interface	The slot/port number that is associated with the static or dynamically learned MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29).

Release History

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain information.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information for the switch.
show mac-learning domain spb	Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.
show mac-learning domain vxlan	Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning domain l2gre	Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slOriginId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblGroupField
```

show mac-learning domain spb

Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.

show mac-learning domain spb [isid *instance_id* | **serviceid** *service_id* **[isid** *instance_id***]] [sap** *chassis/slot/port:encap* | **bind-sdp** *sdp_id***[:***service_id***]] [dynamic | static] [mac-address** *mac_address***] [summary]**

Syntax Definitions

instance_id	A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network. The valid range is 256–16777214.
service_id	An existing SPB service ID.
chassis/slot/port:encap	The SPB access port and encapsulation (**0**, **all**, *qtag*, or *outer_qtag.inner_qtag*) for an SPB Service Access Point (SAP). For example, 1/1/2:10.
mesh_id	A SPB service distribution point (SDP) ID.
*sdp_id***[:***service_id***]**	Displays MAC addresses learned on an SPB Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
dynamic	Displays dynamically learned MAC addresses.
static	Displays static MAC addresses with a permanent status.
mac_address	A MAC Address (for example, 00:00:39:59:f1:0c).
summary	Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned for the SPB domain are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

Examples

```
-> show mac-learning domain spb summary
Mac Address Table Summary:

   Domain       Static     Static-Multicast       Bmac        Dynamic
------------+------------+------------------+-----------+------------
     SPB              0                   0           0            6

 Total MAC Address In Use  = 6

-> show mac-learning domain spb
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
   SPB             1000:1000  e8:e7:32:11:db:72  dynamic  servicing sap:1/1/13:1000
   SPB             1000:1000  e8:e7:32:40:10:7e  dynamic  servicing  sdp:32867:1000
   SPB             1000:1000  e8:e7:32:00:27:e1  dynamic  servicing  sdp:32904:1000
   SPB             1000:1000  e8:e7:32:00:27:ee  dynamic  servicing  sdp:32904:1000
   SPB             3899:3899  e8:e7:32:42:e0:4d  dynamic  servicing     sap:0/99:99
   SPB             3899:3899  e8:e7:32:42:e0:5c  dynamic  servicing     sap:0/99:99

Total number of Valid MAC addresses above = 6

-> show mac-learning domain spb serviceid 3899
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
   SPB             3899:3899  e8:e7:32:42:e0:4d  dynamic  servicing     sap:0/99:99
   SPB             3899:3899  e8:e7:32:42:e0:5c  dynamic  servicing     sap:0/99:99

Total number of Valid MAC addresses above = 2
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured.
Vlan/ServcId/[ISId/vnID]	The SPB service ID number and the ISID number associated with the SPB service ID.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static, bmac).**
Operation	The disposition of the MAC address (**bridging**, **filtering**, **servicing**).
Interface	The SPB service access point (SAP) associated with the MAC address.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain and service information.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information for the switch.
show mac-learning domain vlan	Displays MAC Address Table information for the VLAN source learning domain.
show mac-learning domain vxlan	Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning domain l2gre	Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblGroupField
   slSvcISID
```

show mac-learning domain vxlan

Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.

show mac-learning domain vxlan [vnid *vxlan_id* | **serviceid** *service_id* **[vnid** *vxlan_id***]] [sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id***[:***service_id***]] [dynamic | static] [mac-address** *mac_address***] [summary]**

Syntax Definitions

vxlan_id	A 24-bit numerical value that identifies a VXLAN segment (a VXLAN network ID). The valid range is 1– 2147483647 (or 000.000.001–255.255.255 in decimal notation format). Use a hyphen to specify a range of IDs (25001-25005).
service_id	An existing VXLAN service ID.
chassis/slot/port:encap	The VXLAN service access port and encapsulation (**0**, **all**, *qtag*, or *outer_qtag.inner_qtag*) for a VXLAN Service Access Point (SAP). For example, 1/1/2:10.
*sdp_id***[:***service_id***]**	Displays MAC addresses learned on a VXLAN Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
dynamic	Displays dynamically learned MAC addresses.
static	Displays static MAC addresses with a permanent status.
mac_address	A MAC Address (for example, 00:00:39:59:f1:0c).
summary	Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned for the VXLAN domain are displayed.

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

Examples

```
-> show mac-learning domain vxlan summary
Mac Address Table Summary:

   Domain       Static     Static-Multicast       Bmac        Dynamic
------------+------------+------------------+-----------+------------
   VXLAN               0                  0           0            4

 Total MAC Address In Use  = 4

-> show mac-learning domain vxlan
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
 VXLAN                    5:5 00:0e:1e:06:87:8c  dynamic  servicing     sap:1/1/20A
 VXLAN                    5:5 00:c0:dd:10:2c:c1  dynamic  servicing     sap:1/1/20A
 VXLAN                    5:5 00:0e:1e:0c:58:94  dynamic  servicing       sdp:175:5
 VXLAN                    5:5 46:91:54:dc:6e:41  dynamic  servicing       sdp:175:5

 Total number of Valid MAC addresses above = 4

-> show mac-learning domain vxlan vnid 5 bind-sdp 175
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
 VXLAN                    5:5 00:0e:1e:0c:58:94  dynamic  servicing       sdp:175:5
 VXLAN                    5:5 46:91:54:dc:6e:41  dynamic  servicing       sdp:175:5

 Total number of Valid MAC addresses above = 2
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured.
Vlan/ServcId/[ISId/vnID]	The VXLAN service ID number and VXLAN Network ID (VNID) number associated with the VXLAN service ID.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static, bmac).**
Operation	The disposition of the MAC address (**bridging**, **filtering**, **servicing**).
Interface	The VXLAN Service Access Point (SAP) or Service Distribution Point (SDP) associated with the MAC address

Release History

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain and service information.
Release 7.3.4; VXLAN domain parameters and fields added.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information for the switch.
show mac-learning domain vlan	Displays MAC Address Table information for the VLAN source learning domain.
show mac-learning domain spb	Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.
show mac-learning domain l2gre	Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblGroupField
   slVxLanVnID
```

show mac-learning domain l2gre

Displays MAC Address Table information for the Layer 2 Generic Routing Encapsulation (L2 GRE) source learning domain.

show mac-learning domain l2gre {serviceid *service_id* **| sap** *chassis/slot/port:encap* **| bind-sdp** *sdp_id*[:*service_id*] **| vpnid** *vpn_id***} {dynamic | static} [mac-address** *mac_address***] [summary]**

Syntax Definitions

service_id	An existing L2 GRE service ID.
chassis	The chassis identifier.
slot/port:encap	The access port and encapsulation (**0**, **all**, *qtag*, or *outer_qtag.inner_qtag*) for an L2 GRE Service Access Point (SAP).
sdp_id[:*service_id*]	Displays MAC addresses learned on an L2 GRE Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
vpn_id	A tunnel ID that identifies a GRE tunnel VPN.
dynamic	Displays dynamically learned MAC addresses from the specified domain.
static	Displays static MAC addresses from the specified domain.
mac_address	A specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.
summary	Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned in the L2 GRE tunnel domain are displayed.

Platforms Supported

OmniSwitch 6860, 6865, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

Examples

```
-> show mac-learning domain l2gre summary
Mac Address Table Summary:

   Domain       Static     Static-Multicast       Bmac        Dynamic
------------+------------+------------------+-----------+------------
   L2GRE               0                  0           0            4

 Total MAC Address In Use  = 4

-> show mac-learning domain l2gre
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
L2GRE                      5  00:0e:1e:06:87:8c dynamic  servicing  sap:1/1/20A
L2GRE                      5  00:c0:dd:10:2c:c1 dynamic  servicing  sap:1/1/20A
L2GRE                      5  00:0e:1e:0c:58:94 dynamic  servicing  sdp:175:5
L2GRE                      5  46:91:54:dc:6e:41 dynamic  servicing  sdp:175:5

 Total number of Valid MAC addresses above = 4

-> show mac-learning domain l2gre vpnid 5 bind-sdp 175
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
L2GRE                      5  00:0e:1e:0c:58:94 dynamic  servicing  sdp:175:5
L2GRE                      5  46:91:54:dc:6e:41 dynamic  servicing  sdp:175:5

 Total number of Valid MAC addresses above = 2
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured.
Vlan/ServcId/[ISId/vnID]	The L2 GRE service ID number and the GRE tunnel VPN ID number associated with the L2 GRE service ID.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static, bmac).**
Operation	The disposition of the MAC address (**bridging**, **filtering**, **servicing**).
Interface	The L2 GRE tunnel Service Access Point (SAP) or Service Distribution Point (SDP) associated with the MAC address.

Release History

Release 8.4.1.R02; command introduced.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information for the switch.
show mac-learning domain vlan	Displays MAC Address Table information for the VLAN source learning domain.
show mac-learning domain spb	Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.
show mac-learning domain vxlan	Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblGroupField
   slL2GreVpnID
```

show mac-learning domain local

Displays MAC Address Table information for the local service source learning domain.

show mac-learning domain local [serviceid *service_id***] [sap** *chassis/slot/port:encap* **| dynamic | static | mac-address** *mac_address***] [summary]**

Syntax Definitions

service_id	An existing service ID.
chassis/slot/port:encap	The service access port and encapsulation (**0**, **all**, *qtag*, or *outer_qtag.inner_qtag*) for an SPB Service Access Point (SAP). For example, 1/1/2:10.
dynamic	Displays dynamically learned MAC addresses.
static	Displays static MAC addresses with a permanent status.
mac_address	A MAC Address (for example, 00:00:39:59:f1:0c).
summary	Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned for the local domain are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

Examples

```
-> show mac-learning domain local summary
Mac Address Table Summary:

   Domain       Static     Static-Multicast       Bmac        Dynamic
------------+------------+------------------+------------+------------
     LOCAL             1                   0            0            6

 Total MAC Address In Use  = 7
```

```
-> show mac-learning domain local
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
 LOCAL                  1000  e8:e7:32:11:db:72  dynamic  servicing sap:1/1/13:1000
 LOCAL                  1000  e8:e7:32:40:10:7e  dynamic  servicing  sdp:32867:1000
 LOCAL                  1000  e8:e7:32:00:27:e1  dynamic  servicing  sdp:32904:1000
 LOCAL                  1000  e8:e7:32:00:27:ee  dynamic  servicing  sdp:32904:1000
 LOCAL                  3899  e8:e7:32:42:e0:4d  dynamic  servicing     sap:0/99:99
 LOCAL                  3899  e8:e7:32:42:e0:5c  dynamic  servicing     sap:0/99:99
 LOCAL                  2000  00:22:95:11:22:01   static  servicing   sap:1/1/11:10

Total number of Valid MAC addresses above = 7

-> show mac-learning domain local serviceid 3899
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Domain Vlan/SrvcId/[ISId/vnID]   Mac Address      Type    Operation    Interface
------+----------------------+----------------+--------+----------+--------------
 LOCAL                  3899  e8:e7:32:42:e0:4d  dynamic  servicing     sap:0/99:99
 LOCAL                  3899  e8:e7:32:42:e0:5c  dynamic  servicing     sap:0/99:99

Total number of Valid MAC addresses above = 2
```

output definitions

Domain	The domain in which the MAC address was learned or statically configured.
Vlan/ServcId/[ISId/vnID]	The service ID number associated with the MAC address.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status (**dynamic, static, bmac).**
Operation	The disposition of the MAC address (**bridging**, **filtering**, **servicing**).
Interface	The service access point (SAP) associated with the MAC address.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain and service information.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information for the switch.
show mac-learning domain vlan	Displays MAC Address Table information for the VLAN source learning domain.
show mac-learning domain spb	Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.
show mac-learning domain vxlan	Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning domain l2gre	Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacDomain
   slLocaleType
   slOriginId
   slServiceId
   slSubId
   slMacAddressGbl
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblGroupField
   slSvcISID
```

show mac-learning aging-time

Displays the current aging time value for the Source Learning MAC Address Table.

show mac-learning aging-time

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Note that the aging time is the same for all VLANs because it is not configurable on a per-VLAN basis. The aging time value on this platform is a global parameter that applies to all VLANs.

Examples

```
-> show mac-learning aging-time
Mac Address Aging Time (seconds) = 300
```

Release History

Release 7.1.1; command introduced.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
slMacAddressAgingTable
   slMacAgingValue
```

show mac-learning learning-state

Displays the source learning status of a VLAN, port, or link aggregate.

show mac-learning learning-state [vlan *vlan***[**-*vlan2***]** | **port** *chassis/slot/port* **| linkagg** *agg_id***]**

Syntax Definitions

vlan	The VLAN ID number.
-vlan2	The last VLAN ID in a range of VLAN IDs.
chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
agg_id	Specifies the link aggregate identifier.

Defaults

By default, the source learning status for all switch ports and link aggregates is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **port** or **linkagg** keywords along with the port ID and link aggregate ID to display the source learning status for a specific port or link aggregate ID.
- Use the **vlan** keyword along with the VLAN ID or a range of VLAN IDs to display the source learning status for the specified VLAN or range of VLANs.
- Output display for a range of port IDs is supported with this command. However, output display for a range of link aggregate IDs is not supported.
- When the source learning status is configured for a link aggregate ID, it affects all the ports that are members of the link aggregate. However, the source learning status cannot be configured on individual ports which are members of the link aggregate.

Example

```
-> show mac-learning learning-state

port  source-learning
-----+----------------
1/1    disabled
1/2    enabled
1/3    disabled
```

```
-> show mac-learning learning-state port 1/2

port  source-learning
-----+---------------
1/2    enabled

-> show mac-learning learning-state linkagg 10

port  source-learning
-----+---------------
0/10     disabled
```

output definitions

port	The slot/port number for a switch port or a link aggregate ID number. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29).
source-learning	The source learning status of the port or link aggregate (**enabled** or **disabled**). Configured through the **mac-learning** command.

```
-> show mac-learning learning-state vlan 1-5

    Vlan        Learning State
------------+--------------------
       1         Enabled
       5         Enabled
```

output definitions

Vlan	The VLAN ID numbers of the VLANs that are active.
Learning State	The MAC learning state of the VLANs.

Release History

Release 7.1.1; command introduced

Related Commands

mac-learning	Configures the status of source MAC address learning on a single port, a range of ports or on a link aggregate of ports.

MIB Objects

```
slMacAddressTable
   slMacLearningControlTable
   slMacLearningControlEntry
   slMacLearningControlStatus
```

show mac-learning mode

Displays the current source learning mode (centralized or distributed) for the switch.

show mac-learning mode

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

N/A

Examples

```
-> show mac-learning mode
MAC Learning Mode Configuration = CENTRALIZED
New Configured MAC Learning Mode After Reboot = DISTRIBUTED

-> show mac-learning mode
MAC Learning Mode Configuration = DISTRIBUTED
```

Release History

Release 7.1.1; command introduced.

Related Commands

mac-learning mode	Enables or disables the distributed MAC source learning mode.

MIB Objects

```
slMacAddressTable
   slDistributedMacMode
```

mac-ping

Configure a MAC address ping for testing Layer 2 connectivity.

mac-ping dst-mac *mac_address* **vlan** *vlan_id* **[priority** *vlan_priority***] [drop-eligible** {**true** | **false**}**] [count** *count***] [interval** *delay***] [size** *size***] [isid-check** *isid***]**

Syntax Definitions

mac	The destination MAC address to ping.
vlan-id	The VLAN on which the packets will be sent out.Valid range is 1-4094.
vlan-priority	Specifies both the internal priority of the Mac ping and the 802.1p value on the vlan tag header. Valid range is 0-7.
true | **false**	Specifies both the internal drop precedence of the MAC ping and the CFI bit on the vlan tag header. Default is false.
count	The number of packets to send in one ping iteration.Valid range is 1–5.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is from 100 ms to 1000 ms in multiples of 100 ms.
size	The size of the ICMP payload to be used for the ping iteration. Valid range is 32–1500 bytes.
isid	A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network.

Defaults

parameter	default
vlan-priority	0
drop-eligible	false
count	5
delay	1000 ms
size	36 bytes

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The timeout for each ping request packet is one second. This value is not configurable.
- Destination MAC cannot be a broadcast, multicast, or NULL address.
- Enable the Network Time Protocol (NTP) using the NTP client command for a MAC address ping to work correctly across Virtual Chassis.

Examples

```
-> mac-ping dst-mac 00:11:11:11:11:11 vlan 10
-> mac-ping dst-mac 00:11:11:11:11:11 vlan 10 count 5 size 100
-> mac-ping dst-mac 00:11:11:11:11:11 vlan 1001 isid-check 1002
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

N/A

5 VLAN Management Commands

VLAN management software handles VLAN configuration and the reporting of VLAN configuration changes to other switch tasks. A VLAN defines a broadcast domain that contains physical ports and can span across multiple switches. All switches contain a default VLAN 1. Physical switch ports are initially assigned to VLAN 1 until they are statically or dynamically assigned to other VLANs.

This chapter includes descriptions of VLAN management commands used to create, modify or remove VLANs. These commands allow you to enable or disable Spanning Tree Protocol (STP), add or remove virtual router interfaces, statically assign physical switch ports to a default VLAN, and display VLAN configuration information.

MIB information is as follows:

Filename: ALCATEL-IND1-VLAN-MGR-MIB.mib
Module: alcatelIND1VLANManagerMIB

A summary of the available commands is listed here:

VLAN Management Commands	**vlan** **vlan members untagged** **vlan members tagged** **vlan mtu-ip** **show vlan** **show vlan members**
Private VLAN Commands	**pvlan** **pvlan secondary** **pvlan members** **show pvlan** **show pvlan mapping** **show pvlan members**

vlan

Creates a new VLAN with the specified VLAN ID (VID) and an optional description.

vlan *vlan_id* **[admin-state {enable | disable}] [name** *description***]**

no vlan *vlan_id*

Syntax Definitions

vlan_id	A numeric value that uniquely identifies an individual VLAN. This value becomes the VLAN ID for the new VLAN.
enable	Enable VLAN administrative status.
disable	Disable VLAN administrative status.
description	An alphanumeric string. Optional name description for the VLAN ID.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a VLAN from the configuration.
- All VLAN ports and routers are detached before the VLAN is removed. If the VLAN deleted is a default VLAN on the port, the port returns to default VLAN 1.
- If the VLAN deleted is not a default VLAN, then the ports are directly detached from the VLAN.
- A VLAN is not operationally active until at least one of the member ports of the VLAN is active and can forward traffic.
- Note that specifying multiple VLAN IDs and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range of VLAN ID entries (for example, **vlan 10-15**).
- When a VLAN is administratively disabled, static port assignments are retained but traffic is not forwarded from these ports.
- The description can be any alphanumeric string. Enclose the description in double quotes if it contains more than one word with space in between.

Examples

```
-> vlan 200 name “Corporate VLAN”
-> vlan 720 admin-state disable
-> no vlan 1020
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan members untagged	Statically assigns ports to a VLAN.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanStatus
```

vlan members untagged

Configures a new default VLAN for a single port or an aggregate of ports. The VLAN specified with this command is referred to as the *configured default VLAN* for the port.

vlan *vlan_id***[-***vlan_id***] members {port** *chassis/slot/port***[-***port1***] | linkagg** *agg_id***[-***agg_id***]} untagged**

no vlan *vlan_id***[-***vlan_id***] members {port** *chassis/slot/port***[-***port1***]| linkagg** *agg_id***[-***agg_id***]}**

Syntax Definitions

chassis	The chassis identifier.
vlan_id	An existing VLAN ID number of the VLAN to assign as the default VLAN configured for the port.
*slot/port***[-***port1***]**	The slot number for the module and the physical port number (for example, 3/1 specifies port 1 on slot 3) or a range of physical port numbers on that module (for example, 3/1-16).
*agg_id***[-***agg_id***]**	The link aggregate ID number or range of IDs to be assigned to the specified VLAN.

Defaults

VLAN 1 is the default VLAN for all ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a port or link aggregate from its configured default VLAN and restore VLAN 1 as the default VLAN.
- The VLAN ID and link aggregate ID specified with this command must already exist in the switch configuration.
- This command configures the port or link aggregate to send and receive untagged packets for the specified VLAN ID, which becomes the default VLAN of the port.
- Every switch port or link aggregate has only one configured default VLAN. The 802.1Q tagged ports, however, can have additional VLAN assignments, which are often referred to as *secondary* VLANs.

Examples

```
-> vlan 20 members port 4/1-24 tagged
-> vlan 20 members linkagg 2-4 untagged
-> no vlan 1-4 members port 4/1-24
-> no vlan 20 members linkagg 2-4
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan	Creates a VLAN.
vlan members tagged	Configures a port to accept 802.1q-tagged packets for a specific VLAN.
show vlan	Displays list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
vpaTable
   vpaVlanNumber
   vpaIfIndex
   vpaType
   vpaState
   vpaStatus
```

vlan members tagged

Configures a port or link aggregate ID to send and receive 802.1q-tagged packets with the specified VLAN ID.

vlan *vlan_id***[-***vlan_id***] members {port** *chassis/slot/port***[-***port***] | linkagg** *agg_id***[-***agg_id***]} tagged**

no vlan *vlan_id***[-***vlan_id***] members {port** *chassis/slot/port***[-***port***] | linkagg** *agg_id***[-***agg_id***]}**

Syntax Definitions

vlan_id	The VLAN ID number for a pre-configured VLAN that will handle the 802.1Q-tagged traffic for this port. Use a hyphen to specify a range of VLAN IDs (for example, **vlan 10-15**). The valid range is 1–4094.
chassis	The chassis identifier.
*slot/port***[-***port***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-10).
*agg_id***[-***agg_id***]**	A link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

Defaults

By default, all ports are untagged (they only carry untagged traffic for the default VLAN to which the port belongs).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete 802.1Q tagging on a port or an aggregate of ports.
- The VLAN ID and link aggregate ID specified with this command must already exist in the switch configuration.
- A port or link aggregate cannot be tagged with its own default VLAN ID.

Examples

```
-> vlan 100 members port 3/1 tagged
-> vlan 100 members port 4/1-10 tagged
-> vlan 100 members linkagg 10 tagged
-> vlan 100 members linkagg 1-4 tagged
-> no vlan 100 members port 3/1
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan	Creates a VLAN.
vlan members untagged	Configures the default VLAN for the specified port or link aggregate.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
qPortVlanTable
   qPortVlanSlot
   qPortVlanPort
   qPortVLanStatus
   qPortVlanTagValue
   qPortVlanDescription
   qAggregateVlanTagValue
   qAggregateVlanAggregateId
   qAggregateVlanStatus
   qAggregateVlanDescription
```

vlan mtu-ip

Configures the maximum transmission unit (MTU) packet size allowed for all ports associated with a VLAN. This value is configured on a per VLAN basis, so all IP interfaces assigned to the VLAN apply the same MTU value to packets sent on VLAN ports.

vlan *vlan_id* **mtu-ip** *size*

Syntax Definitions

vlan_id	An existing VLAN ID number of the VLAN to assign as the default VLAN configured for the port.
size	Packet size value specified in bytes.

Defaults

By default, the MTU size is set to 1500 bytes (the standard Ethernet MTU size).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The MTU size applies to traffic sent on all switch ports that are associated with the specified VLAN regardless of the port speed (for example, 10/100 Ethernet, Gigabit Ethernet). Therefore, assign only ports that are capable of handling the MTU size restriction to the VLAN. If the VLAN MTU size is greater than 1500, do not assign 10/100 Ethernet ports to the VLAN.
- By default, packets that exceed the MTU size are dropped. To enable MTU discovery and fragmentation, use the **icmp type** command to enable the “frag needed but DF bit set” control (for example, **icmp type 3 code 4 enable**).
- The maximum MTU size value for a VLAN is 9198.

Examples

```
-> vlan 200 mtu-ip 1280
-> vlan 1503 mtu-ip 9198
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan	Creates a VLAN.
vlan members tagged	Configures a port to accept 802.1q-tagged packets for a specific VLAN.
show vlan	Displays list of existing VLANs.

MIB objects

```
vlanTable
   vlanMtu
```

show vlan

Displays a list of VLANs configured on the switch.

show vlan [*vlan_id***]**

Syntax Definitions

vlan_id	VLAN ID number.

Defaults

By default, a list of all VLANs is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify a VLAN ID with this command to display information about a specific VLAN.
- Note that specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, **show vlan 10-15**). Note that only one VLAN entry - a single VLAN ID or a range of VLAN IDs is allowed with this command. Multiple entries are not accepted.

Examples

```
-> show vlan

 vlan  type  admin  oper  ip   mtu   name
-----+------+-----+-----+-----+-----+------------
1     std     Ena   Dis   Dis  1500   Finance IP
10    unpd    Ena   Dis   Dis  1500   UNP-DYN-VLAN
11    std     Ena   Dis   Dis  1500   VLAN 11
400   spb     Ena   Dis   Dis  1524   VLAN 500
500   fcoe    Ena   Dis   Dis  1500   VLAN 500
600   pvlan-p Ena   Dis   Dis  1500   PVLAN 600
601   pvlan-c Ena   Dis   Dis  1500   PVLAN 601
602   pvlan-i Ena   Dis   Dis  1500   PVLAN 602
```

output definitions

vlan	The numerical VLAN ID. Use the **vlan** command to create or remove VLANs.
type	The type of VLAN (**mtp, vcm, std, unpd, spb, fcoe, pvlan-p, pvlan-c, pvlan-i**). This field also displays the VLANs created through other applications, such as Shortest Path Bridging (SPB), VLAN Stacking, Fibre Channel over Ethernet (FCoE), and Private VLANs (PVLAN).
admin	VLAN administrative status: **Ena** specifies that VLAN functions are enabled; **Dis** specifies that VLAN functions are disabled. Use the **vlan** command to change the VLAN administrative status.

output definitions (continued)

oper	VLAN operational status: **Ena** (enabled) or **Dis** (disabled). The operational status remains disabled until an active port is assigned to the VLAN. When the operational status is enabled, then VLAN properties (for example router interfaces, Spanning Tree) are applied to ports and traffic flow. A VLAN must have an enabled administrative status before it can become operationally enabled.
ip	IP router interface status: **Ena** (IP interface exists for the VLAN) or **Dis** (no IP router interface exists for the VLAN). Use the **ip interface** command to define an IP router interface for a VLAN.
mtu	Maximum Transmission Unit: Size of largest data packet that the VLAN port can transmit. Configured through the **vlan mtu-ip** command.
name	The user-defined text description for the VLAN. By default, the VLAN ID is displayed if the VLAN description is not specified. Configured through the **vlan** command.

```
-> show vlan 600
Name                    : PVLAN 600,
Type                    : PVLAN Primary vlan,
Administrative State    : enabled,
Operational State       : disabled,
IP Router Port          : disabled,
IP MTU                  : 1500
MAC Tunneling           : disabled,
```

output definitions

Name	The user-defined text description for the VLAN. By default, the VLAN ID is displayed if the VLAN description is not specified.
Type	The type of VLAN (such as **Static VLAN, MTP VLAN, VCM IPC, VIP VLAN, UNP Dynamic VLAN, Backbone VLAN, Fibre Channel over Ethernet VLAN**, **PVLAN Primary vlan**)
Administrative State	VLAN administrative status: **enabled** VLAN functions are enabled; **disabled** specifies that VLAN functions are disabled. Use the **vlan** command to change the VLAN administrative status.
Operational State	VLAN operational status: **enabled** or **disabled**. The operational status remains disabled until an active port is assigned to the VLAN. When the operational status is enabled, then VLAN properties (for example router interfaces, Spanning Tree) are applied to ports and traffic flow.
IP Router Port	IP router port status: **enabled** (IP interface exists for the VLAN) or **disabled** (no IP router interface exists for the VLAN). Use the **ip interface** command to define an IP router interface for a VLAN.
IP MTU	Maximum Transmission Unit: Size of largest data packet that the VLAN port can transmit.
MAC Tunneling	MAC tunneling status for the VLAN Stacking SVLAN: **enabled** or **disabled**. Use the **ethernet-service svlan mac-tunneling** to change the MAC tunneling status for the SVLAN.

Release History

Release 7.1.1; command introduced.
Release 8.6R1; “MAC Tunneling” field added.

Related Commands

show vlan members	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanRouterStatus
   vlanType
   vlanMtu
   vlanMacTunneling
```

show vlan members

Displays VLAN-port associations (VPAs) for all VLANs, a specific VLAN, or for a specific port.

show vlan [*vlan_id***[-***vlan_id***]] members [port** *chassis/slot/port***[-***port***]| linkagg** *agg_id***[-***agg_id***]]**

Syntax Definitions

vlan_id	VLAN ID number. Use a hyphen to specify a range of VLAN IDs (for example, **vlan 10-15**).
chassis	The chassis identifier.
*slot/port***[-***port***]**	The slot and port number (3/1) of a specific interface to display. Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id***]**	Enter a link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

Defaults

If no parameters are specified with this command, a list of all VLANs and their assigned ports is displayed by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the *vlan_id* is specified without a *slot/port* or *agg_id*, then all port assignments for that VLAN are displayed.
- If the *slot/port* or *agg_id* is specified without a *vlan_id*, then all VLAN assignments for that port are displayed.
- If both the *vlan_id* and *slot/port* or *agg_id* are specified, then information only for that VLAN and slot/port or link aggregate ID is displayed.
- Note that specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, **show vlan 10-15 port**). Note that only one VLAN entry - a single VLAN ID or a range of VLAN IDs is allowed with this command. Multiple entries are not accepted.
- The following types of VPAs may appear in the “type” field based on the switch configuration:

VPA Type	Description
default	Statically configured default VLAN assignment for the port.
qtagged	Statically configured 802.1Q tagged secondary VLAN assignment for the port.
dynamic	VPA created dynamically as learned by MVRP.
mirror	Port is mirroring the VLAN assignment of another port created according to rules/policies.

VPA Type	Description
mirrored	VPA created dynamically for remote port mirroring.
spb	Port is associated with a Shortest Path Bridging (SPB) Backbone VLAN (BVLAN). When a port is configured as an SPB interface, the port is dynamically assigned to all BVLANs in the switch configuration.
UNP Untagged	Untagged VPA created dynamically for UNP.
UNP QTagged	802.1Q tagged VPA created dynamically for UNP.

Examples

```
-> show vlan members
 vlan   port     type      status
+-----+-------+---------+------------+
  1      1/1    default   inactive
  2      1/2    default   blocking
        11/4    qtagged   forwarding
  3      1/2    qtagged   blocking
        11/4    default   forwarding
         2/5    dynamic   forwarding

-> show vlan 10 members
  port   type      status
+------+--------+------------+
  1/1   default   forwarding
  1/2   qtagged   forwarding

-> show vlan members port 3/2
 vlan     type      status
+------+---------+------------+
   1     default   forwarding
   2     qtagged   forwarding
   5     dynamic   blocking
   3     qtagged   blocking

-> show vlan 1-11 members port 1/3
type       : default,
status     : inactive,
vlan admin : enabled,
vlan oper  : disabled,
```

output definitions

vlan	Numerical VLAN ID. Identifies the VLAN assignment of the port.
port	The slot number for the module and the physical port number on that module (for example 3/1 specifies port 1 on slot 3).
type	The type of VPA: **default** (configured default VLAN assignment for the port), **qtagged** (802.1Q-tagged secondary VLAN assignment for the port), **mirror** (port is mirroring the VLAN assignment of another port), **dynamic (**dynamically configured VLAN assignment for the port).

output definitions

status	The VPA status: **inactive** (port is not active), **forwarding** (traffic is forwarding on this VPA), **blocking** (traffic is not forwarding on this VPA)
vlan admin	VLAN administrative status: **enabled** enables VLAN functions to operate; **disabled** disables VLAN functions without deleting the VLAN. Use the **vlan** command to change the VLAN administrative status.
vlan oper	VLAN operational status: **enabled** or **disabled**. The operational status remains disabled until an active port is assigned to the VLAN. When the operational status is enabled, then VLAN properties (for example router interfaces, Spanning Tree) are applied to ports and traffic flow. A VLAN must have an enabled administrative status before it can become operationally enabled.

Release History

Release 7.1.1; command introduced.

Related Commands

show vlan	Displays list of VLANs configured on the switch.
show ip interface	Displays IP router information.

MIB Objects

```
vlanMgrVpa
vpaTable
   vpaVlanNumber
   vpaIfIndex
   vpaType
   vpaState
   vpaStatus
vlanMgrVlan
vlanTable
   vlanAdmStatus
   vlanOperStatus
```

pvlan

Creates a new Private VLAN (PVLAN) with the specified VLAN ID and an optional description. The specified VLAN ID will serve as the Primary VLAN for the PVLAN configuration.

pvlan *vlan_id***[-***vlan_id***] [admin-state {enable | disable}] [name** *description***] mtu-ip** *size*

no pvlan *vlan_id***[-** *vlan_id***]**

Syntax Definitions

vlan_id	A numeric value that uniquely identifies the PVLAN. The valid range 2–4094.
enable	Enable the VLAN administrative status.
disable	Disable VLAN administrative status.
description	An alphanumeric string. Optional name description for the PVLAN.
size	The Maximum Transfer Unit (MTU) size for the PVLAN.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Specify a VLAN ID that does not already exist in the switch configuration.
- Use a hyphen to indicate a contiguous range of VLAN ID entries.
- Enclose the description in double quotes if it contains more than one word with a space in between each word.

Examples

```
-> pvlan 200 name “Corporate PVLAN”
-> pvlan 200 admin-state disable
-> pvlan 300-302 admin-state enable
-> no pvlan 200
```

Release History

Release 8.3.1; command introduced.

Related Commands

pvlan secondary	Creates a new Secondary VLAN and associates it with the Primary VLAN in a PVLAN configuration.
pvlan members	Assigns ports or link aggregates to a Primary or Secondary VLAN in a PVLAN configuration.
show pvlan	Displays a list of PVLANs configured on the switch.
show pvlan mapping	Displays the Primary VLAN and Secondary VLAN mapping.
show pvlan members	Displays VPAs for all or specific VLANs in a PVLAN configuration.

MIB Objects

```
alaPrivateVlanTable
   alaPrivateVlanID
   alaPrivateVlanAdminState
   alaPrivateVlanName
   alaPrivateVlanType
   alaPrivateVlanMtuIp
```

pvlan secondary

Creates a new Secondary VLAN and associates it with the Primary VLAN in a Private VLAN (PVLAN) configuration.

pvlan *vlan_id* **secondary** *vlan_id***[-***vlan_id***] type {isolated | community}**

no pvlan *vlan_id* **secondary** *vlan_id***[-** *vlan_id***]**

Syntax Definitions

pvlan *vlan_id*	A numeric value that uniquely identifies the Primary VLAN. The valid range is 2–4094.
secondary *vlan_id*	A numeric value that uniquely identifies the Secondary VLAN to assign to the specified Primary VLAN. The valid range is 2–4094.
isolated	Configures the secondary VLAN as an Isolated VLAN.
community	Configures the secondary VLAN as a Community VLAN.

Defaults

parameter	default
N/A	

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of the command to remove the Secondary VLAN assignment.
- The Primary VLAN ID must already exist.
- The Secondary VLAN ID must not already exist.
- Use a hyphen to indicate a contiguous range of VLAN ID entries.
- There can only be one Isolated Secondary VLAN associated with a Primary VLAN.

Examples

```
-> pvlan 200 secondary 250 type isolated
-> pvlan 200 secondary 251 type community
-> no pvlan 200 secondary 251
```

Release History

Release 8.3.1; command introduced.

Related Commands

pvlan	Creates a new Primary VLAN with the specified VLAN ID and an optional description.
pvlan members	Assigns ports or link aggregates to a Primary or Secondary VLAN in a PVLAN configuration.
show pvlan	Displays a list of PVLANs configured on the switch.
show pvlan mapping	Displays the Primary VLAN and Secondary VLAN mapping.
show pvlan members	Displays VPAs for all or specific VLANs in a PVLAN configuration.

MIB Objects

```
alaPrivateVlanMappingTable
   alaPrivateVlanMappingPrimaryVlanID
   alaPrivateVlanMappingSecondaryVlanID
   alaPrivateVlanMappingSecondaryVlanType
```

pvlan members

Configures a tagged or untagged VLAN-port association (VPA) between ports or link aggregates and the specified VLAN ID in a Private VLAN (PVLAN) configuration.

pvlan *vlan_id* **members {port** *chassis/slot/port***[**-*port***] | linkagg** *agg_id***[**-*agg_id***]} {tagged | untagged} | isl}**

no pvlan *vlan_id* **members {port** *chassis/slot/port***[**-*port***] | linkagg** *agg_id***[**-*agg_id***]}**

Syntax Definitions

vlan_id	A numeric value that uniquely identifies a Primary VLAN or Secondary VLAN in a PVLAN configuration. The valid range is 2–4094.
chassis	The chassis identifier.
*slot/port***[**-*port***]**	The slot and port number.
*agg_id***[**-*agg_id***]**	The link aggregate ID number or range of IDs. The ID must be in the range 1 to 128.
tagged	Configures the port or link aggregate ID to send and receive 802.1q-tagged packets with the specified PVLAN ID.
untagged	Configures the port or link aggregate ID to send and receive non-802.1q-tagged packets.
isl	Configures the port as an inter-switch link (ISL) port capable of carrying PVLAN traffic for all the VLANs that are members of a PVLAN between PVLAN-aware switches.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a port or link aggregate from the specified VLAN ID.
- The VLAN ID must already exist in the switch configuration.
- An ISL port can only be assigned to a Primary VLAN.
- When a port is assigned to a PVLAN configuration, the port type is determined by the type of VLAN to which the port is assigned. For example:
  - Ports assigned to a Primary VLAN are designated as promiscuous ports.
  - Ports assigned to a Secondary VLAN configured as a Community VLAN are designated as community ports.
  - Ports assigned to a Secondary VLAN configured as an Isolated VLAN are designated as isolated ports.

- A port or link aggregate can only belong to one Primary VLAN or one Secondary VLAN at any given time. The exception to this is on the OmniSwitch 9900, where multiple VPAs for one port are allowed with the following conditions:
  - Each VLAN tagged on the port must be of the same PVLAN type. For example, port 1/1/2 must belong to either all Primary VLANs, all Isolated Secondary VLANs, or all Community Secondary VLANs.
  - Each VLAN tagged on the port must belong to a different PVLAN domain. For example, porrt 1/1/2 can be tagged with Primary VLAN 200 and Primary VLAN 300 because both VLANs are in separate PVLAN domains.
- Only one untagged VPA is allowed per port.
- On ports with only tagged VPAs, all untagged traffic is dropped.

Examples

```
-> pvlan 200 members port 1/1/1-5 tagged
-> pvlan 200 members linkagg 2-4 untagged
-> pvlan 200 members port 1/1/20 isl
-> no pvlan 200 members port 1/1/1
-> no pvlan 200 members linkagg 2
```

Release History

Release 8.3.1; command introduced.

Related Commands

pvlan	Creates a new Primary VLAN with the specified VLAN ID and an optional description.
pvlan secondary	Creates a new Secondary VLAN that is assigned to a Primary VLAN.
show pvlan	Displays a list of PVLANs configured on the switch.
show pvlan mapping	Displays the Primary VLAN and Secondary VLAN mapping.
show pvlan members	Displays VPAs for all or specific VLANs in a PVLAN configuration.

MIB Objects

```
alaPrivateVlanPortAssociationTable
   alaPrivateVlanPortAssociationVlanID
   alaPrivateVlanPortAssociationPortIfIndex
   alaPrivateVlanPortAssociationVlanOption
   alaPrivateVlanPortAssociationPortType
```

show pvlan

Displays a list of Private VLANs (PVLANs) configured on the switch.

show pvlan [*vlan_id***[-***vlan_id]***]**

Syntax Definitions

vlan_id	PVLAN ID number.

Defaults

By default, a list of all PVLANs is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Specify a VLAN ID with this command to display information about a specific VLAN in a PVLAN configuration.

Examples

```
-> show pvlan
pvlan    type      admin   oper    mtu          name
------+----------+-------+------+------+-----------------
200    Primary    Ena     Dis    1500   PVLAN 200
250    Isolated   Ena     Dis    1500   PVLAN 250
251    Community  Ena     Dis    1500   PVLAN 251
```

output definitions

pvlan	The PVLAN ID.
type	The type of PVLAN (**Primary, Isolated, Community)**
admin	PVLAN administrative status: **Ena** specifies that PVLAN functions are enabled; **Dis** specifies that PVLAN functions are disabled.
oper	PVLAN operational status: **Ena** (enabled) or **Dis** (disabled). The operational status remains disabled until an active port is assigned to the PVLAN. When the operational status is enabled, then PVLAN properties (for example router interfaces, Spanning Tree) are applied to ports and traffic flow. A PVLAN must have an enabled administrative status before it can become operationally enabled.
mtu	The Maximum Transmission Unit size. Specifies the size of the largest data packet that the PVLAN port can transmit.
name	The user-defined text description for the PVLAN. By default, the PVLAN ID is displayed if the PVLAN description is not specified.

```
-> show pvlan 200
Name                    : PVLAN 200,
Type                    : PVLAN Primary vlan,
Administrative State    : enabled,
Operational State       : disabled,
IP MTU                  : 1500
```

output definitions

Name	The user-defined text description for the PVLAN. By default, the PVLAN ID is displayed if the PVLAN description is not specified.
Type	The type of PVLAN (**Primary, Isolated, Community)**
Administrative State	PVLAN administrative status: **enabled** or **disabled**.
Operational State	PVLAN operational status: **enabled** or **disabled**. The operational status remains disabled until an active port is assigned to the PVLAN.
IP MTU	The Maximum Transmission Unit size. Specifies the size of the largest data packet that the PVLAN port can transmit.

Release History

Release 8.3.1; command introduced.

Related Commands

pvlan	Creates a new Primary VLAN with the specified VLAN ID and an optional description.
pvlan secondary	Creates a new Secondary VLAN that is assigned to a Primary VLAN.
show pvlan mapping	Displays the Primary VLAN and Secondary PVLAN mapping.
show pvlan members	Displays VPAs for all or specific VLANs in a PVLAN configuration.

MIB Objects

```
alaPrivateVlanPrimaryVlanID
alaPrivateVlanType
alaPrivateVlanAdminState
alaPrivateVlanOperState
alaPrivateVlan
alaPrivateVlanName
```

show pvlan mapping

Displays the Primary VLAN and Secondary PVLAN mapping in a Private VLAN (PVLAN) configuration.

show pvlan [*vlan_id***] mapping**

Syntax Definitions

vlan_id	PVLAN ID number.

Defaults

If no parameters are specified with this command, the mapping for all PVLANs is displayed by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Specify a VLAN ID with this command to display information about a specific VLAN in a PVLAN configuration.

Examples

```
-> show pvlan mapping
Primary    Secondary
VLAN       VLAN       Type
----------+----------+------------
200        250        Isolated
200        251        Community
```

output definitions

Primary VLAN	The VLAN ID of a Primary VLAN.
Secondary VLAN	The VLAN ID of a Secondary VLAN that is mapped to the Primary VLAN ID.
Type	The type of Secondary VLAN (**Primary, Isolated, Community).**

Release History

Release 8.3.1; command introduced.

Related Commands

pvlan	Creates a new Primary VLAN with the specified VLAN ID and an optional description.
pvlan secondary	Creates a new Secondary VLAN that is assigned to a Primary VLAN.
show pvlan	Displays a list of PVLANs configured on the switch.
show pvlan members	Displays VPAs for all or specific VLANs in a PVLAN configuration.

MIB Objects

```
alaPrivateVlanMappingPrimaryVlanID
alaPrivateVlanMappingSecondaryVlanID
alaPrivateVlanMappingSecondaryVlanType
```

show pvlan members

Displays the VLAN-port associations (VPAs) for all or specific VLANs in a Private VLAN (PVLAN) configuration.

show pvlan [*vlan_id***[-***vlan_id***]] members**

Syntax Definitions

vlan_id	VLAN ID or range of IDs.

Defaults

If no parameters are specified with this command, a list of all PVLANs and their assigned ports is displayed by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Specify a VLAN ID or the range of VLAN IDs with this command to display information about a specific VLAN or for the range of VLAN IDs.

Examples

```
-> show pvlan members
pvlan   port      type               status       port-type
-------+---------+------------------+------------+------------
200     1/10      default            inactive     promiscuous
200     1/11      qtagged            inactive     isl
250     1/15      qtagged            inactive     isolated
251     1/16      default            inactive     community
251     0/10      qtagged            inactive     community

-> show pvlan 200 members
port      type               status       port-type
---------+------------------+------------+------------
1/10      default            inactive     promiscuous
1/11      qtagged            inactive     isl
0/10      qtagged            inactive     promiscuous
```

output definitions

pvlan	The PVLAN ID.
port	The port number.
type	The type of VPA: **default** (configured default VLAN assignment for the port) **qtagged** (802.1Q-tagged secondary VLAN assignment for the port)

output definitions

status	The VPA status: **inactive** (port is not active), **forwarding** (traffic is forwarding on this VPA) **blocking** (traffic is not forwarding on this VPA)
port-type	The PVLAN port type: **Promiscuous**—A port which is a member of a Primary VLAN. **ISL**—A port carrying VLAN traffic for all the VLANs that are members of a PVLAN between "PVLAN-aware" switches. (Isolated, Community, and Promiscuous). **Community—**A port which is a member of a Community VLAN. **Isolated—**A port which is a member of an Isolated VLAN.

Release History

Release 8.3.1; command introduced.

Related Commands

pvlan	Creates a new Primary VLAN with the specified VLAN ID and an optional description.
pvlan secondary	Creates a new Secondary VLAN that is assigned to a Primary VLAN.
pvlan members	Assigns ports or link aggregates to a Primary or Secondary VLAN in a PVLAN configuration.
show pvlan	Displays a list of PVLANs configured on the switch.
show pvlan mapping	Displays the Primary VLAN and Secondary VLAN mapping.

MIB Objects

```
alaPrivateVlanPortAssociationVlanID
alaPrivateVlanPortAssociationPortIfIndex
alaPrivateVlanPortAssociationVlanOption
alaPrivateVlanPortAssociationPortStatus
alaPrivateVlanPortAssociationPortType
```

6 High Availability VLAN Commands

High availability (HA) VLANs send traffic intended for a single destination MAC address to multiple switch ports. The OmniSwitch HA VLAN feature provides an elegant and flexible way to connect server cluster nodes directly to the ingress network. This involves multicasting the service requests on the configured ports. The multicast criteria is configurable based on destination MAC and destination IP address. Egress ports can be statically configured on a server cluster or they can be registered by IGMP reports. The HA VLAN server cluster feature multicasts the incoming packets based on the server cluster configuration on the ports associated with the server cluster.

An HAVLAN is configured by specifying the match criteria, a VLAN and a port list. Match criteria is used to identify the incoming traffic that has to be processed by the HA VLAN server-clusters. The specified VLAN is an ingress and egress VLAN in the case of a L2 server-cluster. In the case of a L3 server-cluster, the VLAN is not configured explicitly, but the IP address specified in the match criteria determines the VLAN. The port list specifies the egress switch ports within the VLAN. The cluster is connected to these switch ports.

There are typically two modes of implementation of server clusters in HA VLAN.

Layer 2 - The server cluster is attached to a L2 switch on which the frames destined to the cluster MAC address are to be flooded on all interfaces.

Layer 3 - The server cluster is attached to a L3 switch on which the frames destined to the server cluster IP address are to be routed to the server cluster IP and then flooded on all interfaces.

For more information, see the application examples in Chapter 28, “Configuring High Availability VLANs” in the *OmniSwitch AOS Release 8 Network Configuration Guide.*

MIB information is as follows:

Filename: ALCATEL-IND1-VLAN-MGR-MIB.mib
Module: alcatelIND1VLANManagerMIB

Filename: ALCATEL-IND1-MAC-ADDRESS-MIB.mib
Module: alcatelIND1MacAddressMIB

A summary of the available commands is listed here:

server-cluster

Configures a cluster with an ID, name, mode and the administrative state.

server-cluster *cluster_id* **[name** *cluster_name***] [mode {L2 | L3}] [admin-state {enable | disable}]**

no server-cluster *cluster_id*

Syntax Definitions

cluster_id	A numerical identifier of the cluster. The valid range is 1–16.
cluster_name	Specifies a name (up to 32 characters) to represent the cluster.
L2	Specifies L2 for the cluster mode.
L3	Specifies L3 for the cluster mode.
enable	Enables the administrative state of the cluster.
disable	Disables the administrative state of the cluster.

Defaults

parameter	default
mode	**L2**
admin-state	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use **no** form of this command to remove the cluster ID from the switch configuration.
- Once the cluster mode is set, the mode cannot be changed.
- Use the **admin-state disable** parameter option to disable an existing cluster before attempting to modify any of the cluster parameters.

Examples

```
-> server-cluster 1
-> server-cluster 1 mode l2
-> server-cluster 1 name l2_cluster mode l2
-> server-cluster 2 name l3_cluster mode l3
-> no server-cluster 1
```

Release History

Release 7.2.1; command was introduced.

Related Commands

vlan	Creates and deletes VLANs.
server-cluster mac-address	Configures a MAC address, VLAN of the specified cluster.
server-cluster port	Configures the specified IP, ARP entry to a given cluster and/or a multicast IP.
show server-cluster	Displays the clusters configured in the system.

MIB Objects

```
alaHAVlanClusterTable
   alaHAVlanClusterId
   alaHAVlanClusterName
   alaHAVlanClusterAdminStatus
   alaHAVlanClusterMode
   alaHAVlanClusterRowStatus
```

server-cluster vlan

Configures a VLAN assignment for the specified cluster. This command is used to assign VLANs to an L2 cluster.

server-cluster *cluster_id* **vlan** *vlan_id*

Syntax Definitions

cluster_id	The numerical identifier of an existing server cluster.
vlan_id	The VLAN identifier to assign to the cluster. The valid range is 1–4094.

Defaults

NA

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- If the specified VLAN ID does not exist in the switch configuration, the cluster will remain operationally disabled.
- Modifying the existing VLAN assignment for a cluster is only allowed when the cluster is administratively disabled.

Examples

```
-> server-cluster 1 vlan 10
-> server-cluster 5 vlan 10
-> server-cluster 6 mac-address 00 :11 :22 :33 :44 :55
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster ip	Configures the specified IP, ARP entry to a given cluster.
server-cluster port	Configures the specified IP, ARP entry to a given cluster and/or a multicast IP.
show server-cluster	Displays the clusters configured in the system.
show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
alaHAVlanClusterTable
   alaHAVlanClusterId
   alaHAVlanClusterVlan
   alaHAVlanClusterMacAddress
   alaHAVlanClusterRowStatus
```

server-cluster mac-address

Configures a MAC address assignment for the specified cluster. This command is used to assign a MAC address to an L2 cluster.

server-cluster *cluster_id* **mac-address** *mac_address*

Syntax Definitions

cluster_id	The numerical identifier of an existing server cluster.
mac_address	The MAC address of the cluster.

Defaults

NA

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- Modifying the existing MAC address assignment for a cluster is only allowed when the cluster is administratively disabled.
- The MAC address that is assigned to a cluster can be a unicast, L2 multicast, or IP multicast address. However reserved multicast MAC addresses cannot be assigned to the cluster.
- The multicast addresses within the following reserved ranges are not supported:
  - 01:00:5E:00:00:00 to 01:00:5E:7F:FF:FF
  - 01:80:C2:XX.XX.XX
  - 33:33:XX:XX:XX:XX

Examples

```
-> server-cluster 1 vlan 10 mac-address 00 :11 :22 :33 :44
-> server-cluster 5 vlan 10
-> server-cluster 5 mac-address 01:
-> server-cluster 6 mac-address 00 :11 :22 :33 :44 :55
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster ip	Configures the specified IP, ARP entry to a given cluster.
server-cluster port	Configures the port or linkagg to be assigned to a specific cluster.
show server-cluster	Displays the clusters configured in the system.
show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
alaHAVlanClusterTable
   alaHAVlanClusterId
   alaHAVlanClusterVlan
   alaHAVlanClusterMacAddress
   alaHAVlanClusterRowStatus
```

server-cluster ip

Configures an IP address and ARP entry for the specified cluster. This command is used to assign an IP address to an L3 cluster.

server-cluster *cluster_id* **ip** *ip_address* **[mac-address {static** *mac_address* **| dynamic}]**

Syntax Definitions

cluster_id	The numerical identifier of an existing server cluster.
ip_address	The unicast IP address to assign to the cluster.
mac_address	The MAC address for the static ARP entry.
dynamic	Dynamically resolve the ARP entry for the cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- A cluster can be assigned an IP address and ARP entry MAC address. Each cluster should have a unique IP address.
- Reserved MAC address cannot be configured as an ARP.
- Modifying the existing IP address parameters for a cluster is only allowed when the cluster is administratively disabled.

Examples

```
-> server-cluster 1 ip 10.135.33.203 mac-address static 00 :11 :22 :33 :44
-> server-cluster 3 ip 10.135.33.205 mac-address dynamic
-> server-cluster 5 ip 10.135.33.207
-> server-cluster 6 mac-address dynamic
-> server-cluster 7 mac-address static 00 :11 :22 :33 :44
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster mac-address	Configures a MAC address of the specified cluster.
server-cluster port	Configures the port or linkagg to be assigned to a specific cluster.
show server-cluster	Displays the clusters configured in the system.

MIB Objects

```
alaHAVlanClusterTable
   alaHAVlanClusterId
   alaHAVlanClusterIfIndex
   alaHAVlanClusterInetAddressType
   alaHAVlanClusterInetAddress
   alaHAVlanClusterMacAddressType
   alaHAVlanClusterMacAddress
   alaHAVlanClusterMulticastStatus
   alaHAVlanClusterMulticastInetAddressType
   alaHAVlanClusterMulticastInetAddress
   alaHAVlanClusterRowStatus
```

server-cluster igmp mode

Configures the IGMP mode status for specified cluster.

server-cluster *cluster_id* **igmp-mode {enable | disable}**

Syntax Definitions

cluster_id	The numerical identifier of an existing server cluster.
enable	Enables IGMP mode for cluster ports.
disable	Disables IGMP mode for cluster ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- When the IGMP mode is enabled for the cluster, the port list is dynamically learned using the IGMP protocol for the configured IP multicast address.
- For HA VLAN IGMP to work, IGMP must be enabled globally on the switch using the command **ip multicast admin-state enable** command.

Examples

```
-> server-cluster 4 igmp-mode enable
-> server-cluster 4 igmp-mode disable
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster ip	Configures the specified IP, ARP entry to a given cluster.
show server-cluster	Displays the clusters configured in the system.

MIB Objects

```
alaHAVlanClusterTable
   alaHAVlanClusterId
   alaHAVlanClusterIfIndex
   alaHAVlanClusterInetAddressType
   alaHAVlanClusterInetAddress
   alaHAVlanClusterMacAddressType
   alaHAVlanClusterMacAddress
   alaHAVlanClusterMulticastStatus
   alaHAVlanClusterMulticastInetAddressType
   alaHAVlanClusterMulticastInetAddress
   alaHAVlanClusterRowStatus
```

server-cluster ip-multicast

Configures a multicast IP address for the specified cluster. This command configures an IP multicast address for an L3 cluster.

server-cluster *cluster_id* **ip-multicast** *ipm_address*

Syntax Definitions

cluster_id	The numerical identifier of an existing server cluster.
ipm_address	The multicast IP address to assign to the cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- A cluster can be assigned an IP address an ARP entry MAC address. Each cluster should have a uniqueIP-address. IP address is configurable only for L3 clusters
- Cluster parameters like IP, multicast IP and MAC address can be modified only when the cluster admin status is disabled.

Examples

```
-> server-cluster 2 ip-multicast 226.0.0.12
-> server-cluster 4 ip-multicast 226.0.0.14
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster	Configures cluster parameters to create or modify a cluster ID.
show server-cluster	Displays the clusters configured in the system.

MIB Objects

```
alaHAVlanClusterTable
   alaHAVlanClusterId
   alaHAVlanClusterIfIndex
   alaHAVlanClusterInetAddressType
   alaHAVlanClusterInetAddress
   alaHAVlanClusterMacAddressType
   alaHAVlanClusterMacAddress
   alaHAVlanClusterMulticastStatus
   alaHAVlanClusterMulticastInetAddressType
   alaHAVlanClusterMulticastInetAddress
   alaHAVlanClusterRowStatus
```

server-cluster port

Configures a port port assignment for the port list of the specified cluster.

server-cluster *cluster_id* **port {***chassis/slot/port***[-***port2***] | all}**

no server-cluster *cluster-id* **port {***chassis/slot/port***[-***port2***] | all}**

Syntax Definitions

cluster_id	The numerical identifier of an existing server cluster.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number to assign to the cluster port list. Use a hyphen to specify a range of ports (1/15-20).
all	Assigns all of the ports that belong to the associated VLAN and NOT all ports on the NI. This parameter applies only to L3 clusters.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to remove a port from the specified cluster port list.
- The cluster ID specified with this command must already exist in the switch configuration.
- Using a port list is not valid for a cluster operating with IGMP mode enabled.
- The **all** parameter does not apply to L2 clusters.

Examples

```
-> server-cluster 1 port 1/21
-> server-cluster 2 port 1/21-23
-> server-cluster 5 port all
-> no server-cluster 1 port 1/21
-> no server-cluster 2 port 1/21-23
-> no server-cluster 3 port all
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster	Configures cluster parameters to create or modify a cluster ID.
show server-cluster	Displays the clusters configured in the system.
show mac-learning	Displays Source Learning MAC Address table information.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
alaHAVlanClusterPortTable
   alaHAVlanClusterId
   alaHAVlanClusterPortIfIndex
   alaHAVlanClusterPortRowStatus
```

server-cluster linkagg

Configures a link aggregate assignment for the port list of the specified cluster.

server-cluster *cluster_id* **linkagg** *agg_id***[-***agg_id2***]**

no server-cluster *cluster_id* **linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

cluster_id	The numerical identifier of an existing server cluster.
*agg_id***[-***agg_id2***]**	The link aggregate ID number to assign to the cluster port list. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to remove a link aggregate ID from the specified cluster port list.
- The cluster ID and link aggregate ID specified with this command must already exist in the switch configuration.
- Using a port list is not valid for a cluster operating with IGMP mode enabled.

Examples

```
-> server-cluster 3 linkagg 1
-> server-cluster 4 linkagg 1-3
-> no server-cluster 3 linkagg 1
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster	Configures cluster parameters to create or modify a cluster ID.
show server-cluster	Displays the clusters configured in the system.
show mac-learning	Displays Source Learning MAC Address table information.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
alaHAVlanClusterPortTable
   alaHAVlanClusterId
   alaHAVlanClusterPortIfIndex
   alaHAVlanClusterPortRowStatus
```

show server-cluster

Displays the cluster configuration information for the switch. If the cluster configuration is set up to run over a Multi-Chassis Link Aggregation (MCLAG) configuration, this command also provides the status of the MCLAG link for the specified cluster.

show server-cluster [*cluster_id* **[port]]**

Syntax Definitions

cluster_id	The numerical identifier of an existing server cluster.
port	Displays the ports and/or link aggregates assigned to a specific cluster.

Defaults

Displays a list of all server clusters configured for the switch.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Specify a cluster ID with this command to display information for a single cluster.
- Use the **port** parameter with the *cluster_id* parameter to display information about the ports assigned to the specified cluster.
- An asterisk (*) is displayed to indicate invalid cases, as shown in the command example.

Examples

```
-> show server-cluster
Legend:   * = operational state: disabled
Cluster Id Mode Vlan   Mac Address      Ip Address   IGMP Address Loopback Status Name
----------+----+----+-----------------+------------+------------+--------------+------
* 10       L2   100  01:10:11:22:33:44     -             -         N/A           c-1
  11       L2   100  01:10:11:22:33:44     -             -         N/A           c-2
  12       L2   100  01:10:11:22:33:44     -             -         N/A           -
  13       L3    -   01:12:11:22:33:44 10.135.33.203     -         Disabled      -
* 14       L3    -   01:12:11:22:33:45 10.135.33.203     -         Disabled      -
  15       L3    -   01:00:6e:00:00:44 10.135.33.203  225.0.1.2    Disabled      c3igmp

-> show server-cluster 10 port
Legend: * = not valid
Cluster ID  Port    Port Type
----------+-------+--------------
* 10       1/3         Static
  10       1/21        Static
* 10       0/2         Static
```

```
-> show server-cluster 11 port
Legend: * = not valid
Cluster ID  Port    Port Type
----------+-------+--------------
10         1/3         Dynamic
10         1/21        Dynamic
10         0/2         Dynamic
```

output definitions

Cluster	The numerical identifier of a cluster.
Mode	Displays the cluster mode as **L2** or **L3**.
Vlan	Displays the VLAN identifier of the cluster.
MAC-Address	The MAC address associated with the cluster.
IP Address	The IP address associated with the cluster.
IGMP Address	The IGMP address associated with the cluster.
Loopback Status	The status of Loopback for the cluster, **Enabled** or **Disabled.**
Name	The name representing the cluster.
Port	Displays the port list of the cluster.
Port Type	Displays the port type, **Static** or **Dynamic**.

```
-> show server-cluster 10
Cluster Id                        : 10,
Cluster Name                      : c-1,
Cluster Mode                      : L2,
Cluster Vlan                      : 100,
Cluster Mac-Address               : 01:10:11:22:33:44,
Administrative State              : Enabled,
Operational State                 : Disabled,
Operational Flag                  : VPA is not forwarding
Multi-Chassis Status              : OutOfSync,
Multi-Chassis OutOfSync Reason    : Multi-Chassis Down,
VFL Status                        : Not-used

-> show server-cluster 15
Cluster Id                        : 15,
Cluster Name                      : c3igmp,
Cluster Mode                      : L3,
Cluster IP                        : 10.135.33.203,
Cluster Mac-Address               : 01:00:6e:00:00:44,
Cluster Mac Type                  : Dynamic,
IGMP-Mode                         : Enabled,
Cluster Multicast IP              : 225.0.1.2,
Loopback Status                   : Disabled,
Administrative State              : Enabled,
Operational State                 : Disabled,
Operational Flag                  : No IGMP reports received
Multi-Chassis Status              : InSync,
Multi-Chassis OutOfSync Reason    : -,
VFL Status                        : Used
```

output definitions

Cluster ID	The numerical identifier of a cluster.
Cluster Name	The name representing the cluster.
Cluster Mode	Displays the cluster mode as **L2** or **L3**.
Cluster IP	The IP address associated with the cluster.
Cluster Mac Type	The type of cluster, **Static** or **Dynamic**.
Cluster Mac-Address	The MAC address associated with the cluster.
IGMP-mode	Specifies the status of IGMP-mode, **Enabled** or **Disabled**.
Cluster Multicast IP	The multicast IP address associated with the cluster.
Loopback Status	The status of Loopback for the cluster, **Enabled** or **Disabled.**
Administrative State	Specifies the administrative status of the cluster, **Enabled** or **Disabled**.
Operational State	Specifies the operational status of the cluster, **Enabled** or **Disabled**.
Operational Flag	Specifies the reason the cluster is operationally down.
Multi-Chassis Status	Whether or not the HAVLAN configuration is consistent between two MCLAG peer switches (**InSync** or **OutOfSync**).
Multi-Chassis OutOfSync Reason	Indicates one of the following reasons the HAVLAN is out of sync between the two MCLAG peer switches: • **Multi-Chassis Down** • **Cluster Operational State Down** • **Server Cluster Mode Mismatch** • **VLAN Mismatch** • **MAC Address Mismatch** • **IP Address Mismatch** • **ARP Type Mismatch** • **IGMP Status Mismatch** • **Multicast IP Address Mismatch** • **All-port Mode Not Supported** • **Sync In Progres** • **Non-VIP-VLAN Not Supported In L3 Mode**
VFL Status	Indicates whether the MCLAG Virtual Fabric Link (VFL) is **Used** or **Not-used** for the cluster.

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R02: **Multi-Chassis Status**, **Multi-Chassis OutOfSync Reason**, **VFL Status** fields added.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
alaHAVlanClusterPortTable
   alaHAVlanClusterId
   alaHAVlanClusterPortIfIndex
   alaHAVlanClusterPortRowStatus
alaHAVlanClusterTable
   alaHAVlanClusterId
   alaHAVlanClusterInetAddress
   alaHAVlanClusterMacAddressType
   alaHAVlanClusterMacAddress
   alaHAVlanClusterMulticastStatus
   alaHAVlanClusterMulticastInetAddress
   alaHAVlanClusterVlan
   alaHAVlanClusterName
   alaHAVlanClusterAdminStatus
   alaHAVlanClusterMode
   alaHAVlanClusterOperStatus
   alaHAVlanClusterOperStatusFlag
   alaHAVlanClusterLoopback
```

7 VLAN Stacking Commands

The VLAN Stacking feature provides a method for tunneling multiple customer VLANs (CVLAN) through a service provider network using one or more service provider VLANs by way of 802.1Q double tagging or VLAN Translation. This feature enables service providers to provide their customers with Transparent LAN Services (TLS). This service is multipoint in nature to support multiple customer sites or networks distributed over the edges of a service provider network.

MIB information for the VLAN Stacking commands is as follows:

Filename: ALCATEL-IND1-E-SERVICE-MIB.mib
Module: alcatelIND1EServiceMIB

Filename: ALCATEL-IND1-VLAN-MGR-MIB.mib
Module: alcatelIND1VLANManagerMIB

A summary of the available commands is listed here:

VLAN Stacking Service Mode	**ethernet-service svlan** **ethernet-service service-name** **ethernet-service nni** **ethernet-service svlan nni** **ethernet-service sap** **ethernet-service sap uni** **ethernet-service sap cvlan** **ethernet-service sap-profile** **ethernet-service sap sap-profile** **ethernet-service uni-profile** **ethernet-service uni-profile inbound 802.1ab** **ethernet-service uni uni-profile** **ethernet-service custom-L2-protocol** **ethernet-service uni-profile custom-L2-protocol** **ethernet-service mac-tunneling** **ethernet-service svlan mac-tunneling** **ethernet-service transparent-bridging** **show ethernet-service vlan** **show ethernet-service** **show ethernet-service sap** **show ethernet-service port** **show ethernet-service nni** **show ethernet-service nni l2pt-statistics** **clear ethernet-service nni l2pt-statistics** **show ethernet-service uni** **show ethernet-service uni l2pt-statistics** **clear ethernet-service uni l2pt-statistics** **show ethernet-service uni-profile** **show ethernet-service custom-l2-protocol** **show ethernet-service uni-profile l2pt-statistics** **clear ethernet-service uni-profile l2pt-statistics** **show ethernet-service mac-tunneling** **show ethernet-service sap-profile**
Wire-rate Hardware Loopback Test	**loopback-test** **show loopback-test** **clear loopback-test counters**

ethernet-service svlan

Creates a VLAN Stacking VLAN (SVLAN) for tunneling customer traffic.

ethernet-service svlan {*svlan_id***[-***svlan_id2***]} [admin-state {enable | disable}] [name** *description***]**

no ethernet-service svlan {*svlan_id* **[-***svlan_id2***]}**

Syntax Definitions

*svlan_id***[-***svlan_id2***]**	The VLAN ID number identifying the SVLAN. Use a hyphen to specify a range of VLAN IDs (10-12).
enable	Enables the SVLAN administrative status.
disable	Disables the SVLAN administrative status, which blocks all ports bound to that SVLAN.
description	An alphanumeric string. Use quotes around the string if the VLAN name contains multiple words with spaces between them (for example, “ALE Engineering”).

Defaults

By default, the Spanning Tree status is enabled in both the **per-vlan** and **flat** mode when the SVLAN is created

parameter	default
enable | disable	**enable**
description	VLAN ID number

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to delete an SVLAN or a range of SVLANs. Note that SVLAN port associations are also removed when the SVLAN is deleted.
- This command does not work if the *svlan_id* specified already exists as a standard VLAN.

Note. Spanning Tree status for an SVLAN only applies to the Spanning Tree topology calculations for the service provider network. This status is not applied to customer VLANs (CVLANs) and does not affect the customer network topology.

Examples

```
-> ethernet-service svlan 1001-1005 admin-state enable name “Customer ABC”
-> no ethernet-service svlan 1001
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ethernet-service vlan	Displays a list of SVLANs configured from the switch

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanType
   vlanAdmStatus
   vlanStatus
```

ethernet-service service-name

Creates a VLAN Stacking service and associates the service with an SVLAN. A service can be carried only on a single SVLAN. All traffic within the associated service is carried on the SVLAN.

ethernet-service service-name *service_name* **svlan** *svlan_id*

no ethernet-service service-name *service_name* **svlan** *svlan_id*

Syntax Definitions

service_name	The name of the VLAN Stacking service; an alphanumeric string. Use quotes around string if the service name contains multiple words with spaces between them (for example, “ALE Engineering”).
svlan_id	The VLAN ID number that identifies an existing SVLAN to associate with the VLAN Stacking service.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to remove a VLAN Stacking service. Note that when a service is removed, the SVLAN association with that service is also removed.
- If the VLAN Stacking service is associated with a Service Access Point (SAP), then remove the SAP associations before attempting to remove the VLAN Stacking service.
- Each VLAN Stacking service is associated with one SVLAN. Specifying an additional VLAN ID for an existing service is not allowed.

Examples

```
-> ethernet-service service-name Marketing svlan 10
-> no ethernet-service service-name Marketing svlan 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service svlan	Creates an SVLAN for customer traffic, a management VLAN for provider traffic for multicast traffic.

MIB Objects

```
alaEServiceTable
   alaEServiceID
   alaEServiceSVLAN
   alaEServiceRowStatus
```

ethernet-service nni

Configures a switch port or link aggregate as a VLAN Stacking Network Network Interface (NNI) and optionally specifies the vendor TPID value and the legacy BPDU processing status for a VLAN Stacking Network Network Interface (NNI).

ethernet-service nni {port *chassis/slot/port* **[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} [tpid** *tpid_value***] [[stp | mvrp] legacy-bpdu {enable | disable}]**

no ethernet-service nni {port *chassis/slot/port* **[-***port2***] | linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

chassis	The chassis identifier.
slot/port **[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).
*agg_id***[-***agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (5-10).
tpid_value	Specifies the TPID value of the port.
enable	Enables the specified legacy BPDU support.
disable	Disables the specified legacy BPDU support.

Defaults

parameter	default
tpid_value	0x8100
stp legacy-bpdu enable | disable	**disable**
mvrp legacy-bpdu enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to revert the VLAN Stacking NNI port or link aggregate back to a conventional switch port or aggregate.
- When this command is used, the default VLAN for the NNI port is changed to a VLAN reserved by the switch for applications such as VLAN Stacking. The reserved VLAN cannot be configured using standard VLAN management commands.
- NNI ports can be 802.1q tagged with normal VLANs. In this case, the TPID of the packets tagged with a normal VLAN must always be 0x8100 (regardless of the TPID of the NNI port). This allows the NNI port to carry regular 802.1q tagged traffic as well as SVLAN tagged traffic.
- Enable legacy BPDU support only on VLAN Stacking network ports that are connected to legacy BPDU switches. Enabling legacy BPDU between AOS switches can cause flooding or an unstable network.

- If legacy BPDU is enabled on a network port while at same time BPDU flooding is enabled on user ports, make sure that tagged customer BPDUs are not interpreted by intermediate switches in the provider network.
- Note that if the peer switch connected to the VLAN Stacking network port supports the Provider MAC address (STP, 802.1ad/D6.0 MAC), then enabling legacy BPDU support is not required on the network port. Refer to the following table to determine the type of STP MAC used:

STP	
Customer MAC	{0x01, 0x80, 0xc2, 0x00, 0x00, 0x00}
Provider MAC address (802.1ad/D6.0)	{0x01, 0x80, 0xc2, 0x00, 0x00, 0x08}
Provider MAC address (Legacy MAC)	{0x01, 0x80, 0xc2, 0x00, 0x00, 0x00}

- STP legacy BPDU are supported only when the **flat** Spanning Tree mode is active on the switch.

Examples

```
-> ethernet-service 10 nni port 1/1/3-5
-> ethernet-service 255 nni port 1/2/1-5 tpid 88a8
-> ethernet-service 500 nni port 1/1/3-5 stp legacy-bpdu enable
-> no ethernet-service 10 nni port 1/1/3
-> no ethernet-service 255 nni linkagg 12-15
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service svlan nni	Associates a switch port or link aggregate with a SVLAN.

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortType
   alaEServicePortVendorTpid
   alaEServicePortLegacyStpBpdu
   alaEServicePortRowStatus
```

ethernet-service svlan nni

Associates an NNI port with an SVLAN. A network port connects to another provider bridge and carries both customer and provider traffic.

ethernet-service svlan {*svlan_id***[-***svlan_id2***]} nni {port** *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]}**

no ethernet-service svlan {*svlan_id***[-***svlan_id2***]} nni {port** *chassis/slot/port***[-***port2***]** | **linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

*svlan_id***[-***svlan_id2***]**	The VLAN ID number identifying the SVLAN. Use a hyphen to specify a range of VLAN IDs (10-12).
chassis	The chassis identifier.
slot/por **[-***port2***]**	The slot and port number (3/1) of an NNI port. Use a hyphen to specify a range of ports (3/1-5).
*agg_id***[-***agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (5-10).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to remove an association between an NNI port and an SVLAN.
- Only SVLAN IDs are accepted with this command. This SVLAN ID specified must already exist in the switch configuration.
- This command only applies to ports or link aggregates configured as VLAN Stacking NNI ports.
- NNI ports can be tagged with normal VLANs. This allows NNI ports to carry regular 802.1q tagged traffic as well as SVLAN tagged traffic.

Examples

```
-> ethernet-service svlan 10 nni port 1/1/3
-> ethernet-service svlan 255 nni port 1/2/1-5
-> ethernet-service svlan 500 nni linkagg 31-35
-> no ethernet-service svlan 10 nni port 1/1/3
-> no ethernet-service svlan 255 nni port 1/2/5
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service svlan	Creates an SVLAN for tunneling customer traffic.
ethernet-service nni	Configures a switch port or link aggregate as a VLAN Stacking NNI.

MIB Objects

```
alaEServiceNniSvlanTable
   alaEServiceNniSvlanNni
   alaEServiceNniSvlanSvlan
   alaEServiceNniSvlanRowStatus
```

ethernet-service sap

Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking service.

ethernet-service sap *sap_id* **service-name** *service_name*

no ethernet-service sap *sap_id*

Syntax Definitions

sap_id	The SAP ID number identifying the service instance.
service_name	The name of the service to associate with this SAP.

Defaults

The “default-sap-profile” profile is automatically associated with the SAP ID when the SAP is created.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to delete a VLAN Stacking SAP. When a SAP is deleted, all port and CVLAN associations with the SAP are also deleted.
- The service name specified with this command must already exist in the switch configuration. Use the **ethernet-service service-name** command to create a service to associate with the SAP.
- Each SAP ID is associated with only one service; however, it is possible to associate one service with multiple SAP IDs.

Examples

```
-> ethernet-service sap 10 service-name CustomerA
-> no ethernet-service sap 11
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service service-name	Creates a VLAN Stacking service and associates the service with an SVLAN.
ethernet-service sap-profile	Creates a VLAN Stacking SAP profile.
ethernet-service sap sap-profile	Associates a SAP profile with a SAP ID.

MIB Objects

```
alaEServiceSapTable
   alaEServiceSapID
   alaEServiceSapServiceID
   alaEServiceSapProfile
   alaEServiceSapRowStatus
```

ethernet-service sap uni

Configures the switch port as a VLAN Stacking User Network Interface (UNI) and associates the port with a VLAN Stacking Service Access Point (SAP). A UNI port is a customer facing port on which traffic enters the SAP.

ethernet-service sap *sap_id* **uni {port** *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]}**

no ethernet-service sap *sap_id* **uni {port** *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]}**

Syntax Definitions

sap_id	The SAP ID number identifying the service instance.
chassis	The chassis identifier.
slot/por **[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).
*agg_id***[**-*agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (5-10).

Defaults

A switch port or a link aggregate becomes a VLAN Stacking UNI port by default when the port or link aggregate is associated with a VLAN Stacking SAP.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to remove an association between a UNI port and a SAP. Note that when the last SAP association is removed, the UNI port converts back to a conventional switch port.
- Only fixed ports can be configured as UNI ports.
- The SAP ID specified with this command must already exist. Use the **ethernet-service sap** command to create a SAP.
- When this command is used, the default VLAN for the UNI port is changed to a reserved VLAN and all customer traffic received is dropped until the type of traffic for the port is configured using the **ethernet-service sap cvlan** command.

Examples

```
-> ethernet-service sap 10 uni port 1/1/3
-> ethernet-service sap 10 uni port 1/2/1-5
-> ethernet-service sap 10 uni linkagg 31-40
-> no ethernet-service sap 10 uni port 1/2/1-5
-> no ethernet-service sap 10 uni linkagg 31
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking SAP and associates the SAP with a VLAN Stacking SAP profile and service.
ethernet-service uni-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.

MIB Objects

```
alaEServiceSapUniTable
   alaEServiceSapUniSap
   alaEServiceSapUniUni
   alaEServiceSapUniRowStatus
```

ethernet-service sap cvlan

Associates customer VLAN (CVLAN) traffic with a VLAN Stacking Service Access Point (SAP). The parameter values configured with this command are applied to frames received on all SAP UNI ports and determines the type of customer traffic that is accepted on the UNI ports and processed by the service.

ethernet-service sap *sap_id* **cvlan {all** | *cvlan_id***[**-*cvlan_id2***]** | **untagged}**

no ethernet-service sap *sap_id* **cvlan {all** | *cvlan_id***[**-*cvlan_id2***]** | **untagged}**

Syntax Definitions

sap_id	The SAP ID number.
all	Applies the SAP profile to tagged and untagged frames.
*cvlan_id***[**-*cvlan_id2***]**	Applies the SAP profile to frames tagged with the specified CVLAN ID. Use a hyphen to specify a range of CVLAN IDs (for example, 10-12 applies the SAP profile to frames tagged with CVLAN 10, 11, or 12).
untagged	Applies the SAP profile only to untagged frames.

Defaults

By default, no CVLAN traffic is associated with the SAP ID when the SAP is created.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to remove a CVLAN ID or the designation for **all** or **untagged** frames from the SAP. Note that when the last CVLAN parameter is deleted from an SAP configuration, the SAP is not automatically deleted.
- The **all** and **untagged** parameters are configurable in combination with a CVLAN ID. For example, if **untagged** and a CVLAN ID are associated with the same SAP ID, then the SAP profile is applied to only untagged traffic *and* traffic tagged with the specified CVLAN ID. All other traffic is dropped.
- The SAP ID specified with this command must already exist. Use the **ethernet-service sap** command to create a SAP.
- Configuring the **all** and **untagged** parameters for the same SAP is not allowed. Specify only one of these two parameters per SAP.
- Either the **all** or **untagged** parameters can be configured for the SAP. In such an instance, the default VLAN for the UNI ports associated with the SAP is changed to the VLAN assigned to the SAP related service.
- Only one SAP, with the **all** or **untagged** option, is allowed per UNI. For example, if UNI port 1/17 is part of SAP 10 and SAP 20 and SAP 10 is configured for **all** traffic, then only **untagged** parameter or a CVLAN ID is allowed for SAP 20.
- If you do not specify **all** or **untagged** options with a UNI, then the default VLAN 4095 is set for the UNI and all untagged, untagged control traffic and unmatched tag traffic is dropped.

Examples

```
-> ethernet-service sap 10 cvlan 200
-> ethernet-service sap 10 cvlan all
-> ethernet-service sap 11 cvlan 100-150
-> ethernet-service sap 11 cvlan untagged
-> no ethernet-service sap 10 cvlan 200
-> no ethernet-service sap 10 cvlan all
-> no ethernet-service sap 10 cvlan 100-150
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking service.

MIB Objects

```
alaEServiceSapCvlanTable
   alaEServiceSapCvlanSapId
   alaEServiceSapCvlanCvlan
   alaEServiceSapCvlanMapType
   alaEServiceSapRowStatus
```

ethernet-service sap-profile

Creates a profile for a VLAN Stacking Service Access Point (SAP). Profile attributes are used to define traffic engineering policies that are applied to traffic serviced by the SAP.

ethernet-service sap-profile *sap_profile_name* **[bandwidth not-assigned] [[shared | not-shared] ingress-bandwidth** *mbps* **] [cvlan-tag {preserve | translate}] priority [not-assigned | map-inner-to-outer-p | map-dscp-to-outer-p | fixed** *value***][egress-bandwidth** *mbps***]**

no ethernet-service sap-profile *sap_profile_name*

Syntax Definitions

sap_profile_name	An alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).
bandwidth not-assigned	Specifies that the SAP profile does not allocate switch resources to enforce bandwidth requirements. Applies only when the profile specifies the default ingress bandwidth value (zero).
shared	Shares the ingress bandwidth limit across all SAP ports and CVLANs.
not shared	Applies the ingress bandwidth limit to individual SAP ports and CVLANs; bandwidth is not shared.
ingress bandwidth *mbps*	The maximum amount of bandwidth to be allowed for SAP ports, for the incoming traffic, in megabits per second. This parameter can be used only along with the shared option or not-shared option.
preserve	Retains the customer VLAN ID (inner tag) and double tags the frame with the SVLAN ID (outer tag).
translate	Replaces the customer VLAN ID with the SVLAN ID.
priority not-assigned	Specifies that the SAP profile is not assigned with a priority value or priority mapping.
map-inner-to-outer-p	Maps the customer VLAN (inner tag) priority bit value to the SVLAN (outer tag) priority bit value.
map-dscp-to-outer-p	Maps the customer VLAN (inner tag) DSCP value to the SVLAN (outer tag) priority bit value.
fixed *value*	Sets the SVLAN (outer tag) priority bit to the specified value.
egress-bandwidth *mbps*	The maximum amount of bandwidth to be allowed for SAP ports, for the outgoing traffic, in megabits per second. *This parameter is not supported on an OmniSwitch 6900.*

Defaults

parameter	default
shared | not shared	**shared**
mbps	0
preserve | translate	**preserve**
not-assigned | map-inner-to-outer-p | map-dscp-to-outer-p | fixed *value*	**fixed** 0

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to delete a SAP profile.
- If a profile is not specified when a SAP is created, a default profile (default-sap-profile) is automatically associated with the SAP.
- Use the **ethernet-service sap sap-profile** command to associate a profile to a VLAN Stacking SAP.
- Only one SAP profile name is associated with each SAP ID; however, it is possible to associate the same SAP profile name to multiple SAP IDs.
- Configure the **ingress-bandwidth** or **egress-bandwidth** parameters to define rate limiting values for the SAP.

Examples

```
-> ethernet-service sap-profile video1 egress-bandwidth 10 cvlan-tag translate
priority map-inner-to-outer-p
-> ethernet-service sap-profile voice1 not-shared ingress-bandwidth 10 cvlan-tag
preserve
-> ethernet-service sap-profile voice2 shared ingress-bandwidth 10
-> no ethernet-service sap-profile video1
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking SAP and associates the SAP with a service.
ethernet-service sap sap-profile	Associates a SAP profile with a SAP ID.
show ethernet-service sap-profile	Displays the profile attribute configuration for a SAP profile.

MIB Objects

```
alaEServiceSapProfileTable
   alaEServiceSapProfileID
   alaEServiceSapProfileCVLANTreatment
   alaEServiceSapProfileIngressBW
   alaEServiceSapProfileEgressBW
   alaEServiceSapProfilePriorityMapMode
   alaEServiceSapProfileFixedPriority
   alaEServiceSapProfileBandwidthShare
   alaEServiceSapRowStatus
```

ethernet-service sap sap-profile

Associates a VLAN Stacking Service Access Point (SAP) with a SAP profile. This command is also used to change an existing SAP profile association.

ethernet-service sap *sap_id* **sap-profile** *sap_profile_name*

no ethernet-service sap *sap_id*

Syntax Definitions

sap_id	The SAP ID number.
sap_profile_name	The name of the SAP profile to associate with this SAP ID.

Defaults

The “default-sap-profile” profile is automatically associated with the SAP ID when the SAP is created.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command along with the SAP ID to remove the SAP profile.
- If a profile association already exists for the specified SAP ID, the current profile is replaced with the profile specified with this command.
- To change the profile associated with the SAP back to the default profile, enter “default-sap-profile” with this command.
- Do not specify a service name; doing so returns an error message. This command is only for associating an existing profile to a VLAN Stacking SAP.

Examples

```
-> ethernet-service sap 10 sap-profile CustomerC
-> ethernet-service sap 11 sap-profile CustomerD
-> ethernet-service sap 11 sap-profile default-sap-profile
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking SAP and associates the SAP with a VLAN Stacking SAP profile and service.
ethernet-service sap-profile	Creates a VLAN Stacking SAP profile.

MIB Objects

```
alaEServiceSapTable
   alaEServiceSapID
   alaEServiceSapProfile
   alaEServiceSapRowStatus
```

ethernet-service uni-profile

Creates a User Network Interface (UNI) profile that is used to specify how to process control packets ingressing on UNI ports.

ethernet-service uni-profile *uni_profile_name* **[tunnel-mac** *mac_address***] [l2-protocol** *protocol***] {peer | discard | tunnel | mac-tunnel}**

no ethernet-service uni-profile *uni_profile_name*

Syntax Definitions

uni_profile_name	Alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).
mac_address	The tunnel MAC address to use when configuring MAC tunneling. *This parameter is not supported on the OmniSwitch 6900.*
protocol	The protocol to which the specified action is applied. Refer to the table in the “Usage Guidelines” section of this command page for a list of protocol keywords to select.
peer	Allows the UNI port to participate in the specified protocol.
discard	Discards the specified PDU.
tunnel	Tunnels the specified PDU across the provider network.
mac-tunnel	Changes the destination MAC address to either the configured or default tunnel MAC address before forwarding. *This parameter is not supported on the OmniSwitch 6900.*

Defaults

By default, the tunnel MAC address is set to 01:00:0c:cd:cd:d0. Refer to the table in the “Usage Guidelines” section of this command page for the default action settings for each protocol parameter.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to delete a UNI profile. Remove any UNI profile associations with UNI ports before attempting to modify or delete the profile.
- If a user-configured UNI profile is *not* associated with a UNI port, then the default profile (*default-uni-profile*) is used to process control packets ingressing on the port.
- The following table provides the default and supported profile actions for each protocol parameter:

Protocol Keyword	Reserved DA MAC Address	Default Action	peer	discard	tunnel	mac-tunnel
stp	01:80:c2:00:00:00	**tunnel**	no	yes	yes	yes
802.1x	01:80:c2:00:00:03	**discard**	no	yes	yes	yes
802.3ad	01:80:c2:00:00:02	**peer**	yes	yes	yes	yes
802.1ab	01:80:c2:00:00:0e	**discard**	yes	yes	yes	yes
mvrp	01:80:c2:00:00:21	**tunnel**	no	yes	yes	yes
amap	00:20:da:00:70:04	**discard**	no	yes	yes	yes
oam	01:80:c2:00:00:02	**peer**	yes	yes	yes	yes
lacpmarker	01:80:c2:00:00:02	**peer**	yes	yes	yes	yes
udld	01:00:0c:cc:cc:cc	**peer**	yes	yes	yes	yes
pagp	01:00:0c:cc:cc:cc	**discard**	no	yes	yes	yes
cdp	01:00:0c:cc:cc:cc	**discard**	no	yes	yes	yes
vtp	01:00:0c:cc:cc:cc	**discard**	no	yes	yes	yes
dtp	01:00:0c:cc:cc:cc	**discard**	no	yes	yes	yes
pvst	01:00:0c:cc:cc:cd	**discard**	no	yes	yes	yes
vlan	01:00:0c:cd:cd:ce	**discard**	no	yes	yes	yes
uplink	01:00:0c:cd:cd:cd	**discard**	no	yes	yes	yes

- The **oam**, **lacpmarker**, **udld**, **pagp**, **cdp**, **vtp**, **dtp**, **pvst**, **vlan**, and **uplink** protocol keywords are not supported with this command on the OmniSwitch 6900.
- To specify how to process tagged and untagged 802.1AB control frames, use the **ethernet-service uni-profile inbound 802.1ab** command.
- Up to five unique UNI profile combinations, including the default and built-in profiles, are allowed per switch.

Examples

```
-> ethernet-service uni-profile uni_1 l2-protocol mvrp discard
-> ethernet-service uni-profile uni_2 tunnel-mac 01:00:0c:cd:cd:cd l2-protocol pagp
mac-tunnel
-> ethernet-service uni-profile uni_3 l2-protocol uplink tunnel
ERROR: Only 5 profiles are allowed for this type
-> no ethernet-service uni-profile uni_1
-> no ethernet-service uni-profile uni_2
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; **tunnel-mac** address and protocol parameters added, **mac-tunnel** action parameter added.

Related Commands

ethernet-service uni-profile custom-L2-protocol	Assigns a custom L2 protocol MAC address entry to a UNI profile.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
ethernet-service sap uni	Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking Service Access Point (SAP).
show ethernet-service uni	Displays the profile associations for VLAN Stacking UNI ports.
show ethernet-service uni-profile	Displays the profile attribute configuration for VLAN Stacking UNI profiles.

MIB Objects

```
alaEServiceUNIProfileTable
   alaEServiceUNIProfileID
   alaEServiceUNIProfileStpBpduTreatment
   alaEServiceUNIProfile8021xTreatment
   alaEServiceUNIProfile8021ABTreatment
   alaEServiceUNIProfile8023adTreatment
   alaEServiceUNIProfileMvrpTreatment
   alaEServiceUNIProfileAmapTreatment
   alaEServiceUNIProfileVtpTreatment
   alaEServiceUNIProfileVlanTreatment
   alaEServiceUNIProfileUplinkTreatment
   alaEServiceUNIProfileUdldTreatment
   alaEServiceUNIProfilePvstTreatment
   alaEServiceUNIProfilePagpTreatment
   alaEServiceUNIProfileLacpmarkerTreatment
   alaEServiceUNIProfileDtpTreatment
   alaEServiceUNIProfileCdpTreatment
   alaEServiceUNIProfileTunnelMac
   alaEServiceUNIProfileOamTreatment
   alaEServiceUNIProfileRowStatus
```

ethernet-service uni-profile inbound 802.1ab

Configures the treatment of Layer 2 tagged and untagged 802.1AB control frames that are received on UNI ports. Use this command to specify a different action (peer, drop, or tunnel) based on the tagged and untagged state of an 802.1AB control frame.

ethernet-service uni-profile *uni_profile_name* **inbound {tagged | untagged | both} l2-protocol 802.1ab {peer | discard | tunnel}**

no ethernet-service uni-profile *uni_profile_name*

Syntax Definitions

uni_profile_name	Alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).
tagged	The specified action is applied only to tagged 802.1AB control frames.
untagged	The specified action is applied only to untagged 802.1AB control frames.
both	The specified action is applied to both tagged and untagged 802.1AB control frames.
peer	Allows the UNI port to participate in the 802.1AB protocol.
discard	Discards 802.1AB PDUs.
tunnel	Tunnels 802.1AB PDUs across the provider network.

Defaults

By default, tagged and untagged 802.1AB control frames are dropped.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to delete a UNI profile. Remove any UNI profile associations with UNI ports before attempting to modify or delete the profile.
- When only the **tagged** keyword is used, the specified action is applied to tagged traffic and the default action (**discard**) is applied to untagged traffic.
- When only the **untagged** keyword is used, the specified action is applied to untagged traffic and the default action (**discard**) is applied to tagged traffic.
- Only the **tunnel** and **discard** actions can be configured for tagged control frames.
- Only the **peer** and **discard** actions can be configured for untagged control frames.
- The treatment of 802.1AB control frames received on access ports can either be mixed (different for tagged, different for untagged) or the same for both tagged and untagged control frames. To switch between mixed and the same, set the action for tagged and untagged frames back to the default (**discard**).

- Use the **ethernet-service uni-profile** command to configure the treatment for other protocol control frames. This command applies only to 801.1AB frames.

Examples

```
-> ethernet-service uni-profile lldp-tagged inbound tagged l2-protocol 802.1ab
tunnel
-> ethernet-service uni-profile lldp-untagged inbound untagged l2-protocol 802.1ab
peer
-> ethernet-service uni-profile lldp-diff inbound tagged l2-protocol 802.1ab tunnel
inbound untagged l2-protocol 802.1ab peer
-> ethernet-service uni-profile lldp-both inbound both l2-protocol 802.1ab discard

-> no ethernet-service uni-profile lldp-tagged
-> no ethernet-service uni-profile lldp-untagged
-> no ethernet-service uni-profile lldp-diff
-> no ethernet-service uni-profile lldp-both
```

Release History

Release 8.6R2; command introduced.

Related Commands

ethernet-service uni-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
show ethernet-service uni-profile	Displays the profile attribute configuration for VLAN Stacking UNI profiles.

MIB Objects

```
alaEServiceUNIProfileTable
   alaEServiceUNIProfileID
   alaEServiceUNIProfileStpBpduTreatment
   alaEServiceUNIProfile8021xTreatment
   alaEServiceUNIProfile8021ABTreatment
   alaEServiceUNIProfile8023adTreatment
   alaEServiceUNIProfileMvrpTreatment
   alaEServiceUNIProfileAmapTreatment
   alaEServiceUNIProfileVtpTreatment
   alaEServiceUNIProfileVlanTreatment
   alaEServiceUNIProfileUplinkTreatment
   alaEServiceUNIProfileUdldTreatment
   alaEServiceUNIProfilePvstTreatment
   alaEServiceUNIProfilePagpTreatment
   alaEServiceUNIProfileLacpmarkerTreatment
   alaEServiceUNIProfileDtpTreatment
   alaEServiceUNIProfileCdpTreatment
   alaEServiceUNIProfileTunnelMac
   alaEServiceUNIProfileOamTreatment
   alaEServiceUNIProfile8021ABTagTreatment
   alaEServiceUNIProfile8021ABUnTagTreatment
   alaEServiceUNIProfileRowStatus
```

ethernet-service uni uni-profile

Associates a VLAN Stacking User Network Interface (UNI) profile with a UNI port.

ethernet-service uni {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} uni-profile** *uni_profile_name*

Syntax Definitions

chassis	The chassis identifier.
slot/por **[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).
*agg_id***[**-*agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (5-10).
uni_profile_name	Alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

Defaults

The default profile (*default-uni-profile*) is used to process control packets ingressing on a UNI port. This profile is assigned at the time a port is configured as a VLAN Stacking UNI.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- This UNI profile name specified with this command must already exist in the switch configuration.
- To change the profile associated with a UNI port, use this command and specify a different profile name than the one currently associated with the port. The last profile associated with the port, is the profile that is applied to UNI port traffic.
- To change the profile associated with a UNI port back to the default profile, enter “default-uni-profile” with this command.
- On the OmniSwitch 6465, OmniSwitch 6860, and OmniSwitch 6865, there are also two built-in UNI profiles (*ieee-fwd-all* and *ieee-drop-all*) that can be assigned to a UNI port. Use one of the profiles to tunnel or discard all IEEE multicast MAC address traffic received on the UNI port.
  - When a UNI port is assigned to the *ieee-fwd-all* profile, all L2 protocol control packets destined for 01:80:C2:00:00:XX are forwarded as normal data. However, control packets with a destination MAC address of 01:80:C2:00:00:01, 01:80:C2:00:00:04, or 01:80:C2:00:00:08 are not forwarded end-to-end.
  - When a UNI port is assigned to the *ieee-drop-all* profile, all L2 protocol control packets destined for 01:80:C2:00:00:XX are discarded.
  - When a UNI port is assigned to either one of the built-in profiles (*ieee-fwd-all* or *ieee-drop-all*), tunneled L2 protocol control packets (tagged packets with SVLAN ID) received on NNI ports are forwarded as normal data.

Examples

```
-> ethernet-service uni port 1/1/3 uni-profile uni_1
-> ethernet-service uni linkagg 1-5 uni-profile uni_2
-> ethernet-service uni port 1/2/1-5 uni-profile default-uni-profile
-> ethernet-service uni port 1/1/6 uni-profile ieee-fwd-all
-> ethernet-service uni port 1/1/7 uni-profile ieee-drop-all
```

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service uni-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service sap uni	Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking Service Access Point (SAP).

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortType
   alaEServicePortUniProfile
   alaEServiceSapUniRowStatus
```

ethernet-service custom-L2-protocol

Creates a custom L2 protocol MAC address entry with an optional mask, EtherType, or SSAP/DSAP protocol identifier. A custom L2 protocol entry is configured for a proprietary protocol with a destination multicast MAC address and is assigned to a UNI profile for specific packet control.

ethernet-service custom-L2-protocol *custom_protocol_name* **mac** *mac_address* **[mask** *mask* **| ether-type** *ethertype* **[subtype** *subtype***] | ssap/dsap** *ssap/dsap* **pid** *pid***]**

no ethernet-service custom-L2-protocol *name*

Syntax Definitions

custom_protocol_name	An alphanumeric string (up to 32 characters) that identifies the custom L2 protocol entry.
mac_address	A multicast MAC address for the custom L2 protocol entry (for example, 01:80:c2:00:11:11).
mask	A mask defines a range of MAC addresses for the custom L2 protocol MAC address entry (for example, ff:ff:ff:ff:ff:00).
ethertype	An integer value to specify a generic EtherType.
subtype	An integer value to specify a Sub-Type for the EtherType.
ssap/dsap	Source service access point and destination service access point specific to LLC/SNAP in numerical or hexadecimal format.
pid	Protocol identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865

Usage Guidelines

- Use the **no** form of this command to delete the configured custom L2 protocol entry. A custom L2 protocol entry cannot be deleted if the entry is assigned to a UNI profile that is assigned to a UNI port.
- Consider the following command guidelines when configuring a custom L2 protocol:

When configuring a custom L2 protocol with ...	The ...
a MAC address and no mask	MAC address cannot be: • a reserved IPv4/IPv6 multicast address. • a MAC-specific control protocol (01-80-C2-00-00-01 or 01-80-C2-00-00-04). • a Service OAM address (01-80-C2-00-00-30 to 01-80-C2-00-00-3F). • used in another custom L2 protocol without a mask.

When configuring a custom L2 protocol with ...	The ...
a MAC address with a mask	MAC address range cannot overlap with: • reserved IPv4/IPv6 multicast address ranges. • a MAC address range configured for another custom L2 protocol. Only nested ranges are allowed.
an EtherType and optional Sub-Type	The EtherType/Sub-Type value cannot be: • configured if a mask was specified for the MAC address. • configured for another custom L2 protocol. • a well-known L2 protocol ((0x8809/1, 0x8809/2, 0x8809/3, 0x888E, 0x88CC, 0x88F5).
an optional SSAP/DSAP and PID	The SSAP/DSAP PID value cannot be: • configured if a mask or EtherType value was specified for the MAC address. • configured for another custom L2 protocol.

- The MAC address, mask, EtherType, Sub-Type, SSAP/DSAP, and PID cannot be modified once the custom L2 protocol is created. The custom L2 protocol must be deleted and created again with the new values required.
- A custom L2 protocol is assigned to an existing UNI L2 protocol profile using the **ethernet-service uni-profile custom-L2-protocol** command. The action for the custom L2 protocol entry is specified when the entry is assigned to a UNI L2 protocol profile.

Examples

```
-> ethernet-service custom-L2-protocol tunnel-mac mac 01:80:c2:00:11:11
-> ethernet-service custom-L2-protocol tunnel-mac-range mac 01:80:c2:00:11:11 mask
ff:ff:ff:ff:ff:00
-> ethernet-service custom-L2-protocol tunnel-mac-ethertype mac 01:80:c2:00:11:11
ethertype 0x5555
-> ethernet-service custom-L2-protocol tunnel-mac-ethersubtype mac
01:80:c2:00:11:11 ethertype 0x5556 subtype 120
-> ethernet-service custom-L2-protocol tunnel-mac-ssap mac 01:80:c2:00:11:11 ssap/
dsap 43/43 pid 3
-> ethernet-service custom-L2-protocol discard-mac-range mac 01:80:c2:00:11:11 mask
ff:ff:ff:00:ff:ff
```

Release History

Release 8.6R1; command introduced.

Related Commands

ethernet-service uni-profile custom-L2-protocol	Assigns a custom L2 protocol entry to a UNI profile.
show ethernet-service custom-l2-protocol	Displays the custom L2 protocol configuration for the switch.

MIB Objects

```
alaEServiceCustomL2ProtocolTable
   alaEServiceCustomL2ProtocolName
   alaEServiceCustomL2ProtocolMac
   alaEServiceCustomL2ProtocolMask
   alaEServiceCustomL2ProtocolEtherType
   alaEServiceCustomL2ProtocolEtherSubType
   alaEServiceCustomL2ProtocolSsap
   alaEServiceCustomL2ProtocolDsap
   alaEServiceCustomL2ProtocolId
   alaEServiceCustomL2ProtocolRowStatus
```

ethernet-service uni-profile custom-L2-protocol

Assigns a custom L2 protocol entry to a UNI profile.

ethernet-service uni-profile *uni_profile_name* **custom-L2-protocol** *custom_protocol_name* **{tunnel | discard | mac-tunnel}**

no ethernet-service uni-profile *uni_profile_name* **custom-L2-protocol** *custom_protocol_name*

Syntax Definitions

uni_profile_name	Name of the configured UNI profile.
custom_protocol_name	Name of the configured custom L2 protocol entry to assign to the specified UNI profile.
tunnel	Tunnels packets with a destination MAC address that matches the MAC address configured for the custom L2 protocol. The MAC address of the packet is not changed.
discard	Discards packets with a destination MAC address that matches the MAC address configured for the custom L2 protocol.
mac-tunnel	Changes the destination MAC address of a packet to the configured tunnel MAC address for the specified UNP profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865

Usage Guidelines

- Use the **no** form of this command to remove the custom L2 protocol entry from the UNI profile.
- If the specified UNI profile is already assigned to a UNI port, then a custom L2 protocol entry cannot be assigned or deleted from the UNI profile.
- The **tunnel** and **discard** actions apply to all traffic matching a custom L2 protocol entry.
- The **mac-tunnel** action applies only to traffic matching a custom L2 protocol entry that was configured with an EtherType and optional Sub-Type value or an SSAP/DSAP PID value.
- More than one custom L2 protocol entry can be assigned to a UNI profile, but not in the same command line. Configure each custom L2 protocol assignment one at a time; a separate command for each entry.

Examples

```
-> ethernet-service uni-profile uni-prof1 custom-L2-protocol tunnel-mac tunnel
-> ethernet-service uni-profile uni-prof2 custom-L2-protocol tunnel-mac-range
tunnel
-> ethernet-service uni-profile uni-prof3 custom-L2-protocol tunnel-mac-ethertype
```

```
mac-tunnel
-> ethernet-service uni-profile uni-prof4 custom-L2-protocol tunnel-mac-
ethersubtype tunnel
-> ethernet-service uni-profile uni-prof5 custom-L2-protocol tunnel-mac-ssap mac-
tunnel
-> ethernet-service uni-profile uni-prof6 custom-L2-protocol discard-mac-range
discard
-> ethernet-service uni-profile uni-prof6 custom-L2-protocol discard-mac-ethertype
discard
-> ethernet-service uni-profile uni-prof6 custom-L2-protocol discard-mac-ssap
discard
-> ethernet-service uni-profile uni-prof7 custom-l2-protocol tunnel-mac tunnel
ERROR: A profile that is bound to a UNI cannot be modified

-> no ethernet-service uni-profile uni-prof1 custom-L2-protocol tunnel-mac-
ethertype
-> no ethernet-service uni-profile uni-prof7 custom-l2-protocol tunnel-mac
ERROR: UNI Profile must be unused by any UNI port before disassociation of a Custom
L2 Protocol
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ethernet-service uni-profile	Displays the UNI profile configuration for the switch, which includes any custom L2 protocol assignments.

MIB Objects

```
alaEServiceUNIProfileL2CustomProtocolTable
   alaEServiceUNIProfileL2CustomID
   alaEServiceUNIProfileL2CustomProtocolID
   alaEServiceUNIProfileL2CustomProtocolType
   alaEServiceUNIProfileL2CustomProtocolRowStatus
```

ethernet-service mac-tunneling

Configures the global MAC tunneling status. When enabled (the default), MAC tunneling is active for all UNI profile protocols that are configured with the MAC tunneling action.

ethernet-service mac-tunneling {enable | disable}

Syntax Definitions

enable	Globally enables the MAC tunneling status.
disable	Globally disables the MAC tunneling status.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6860, 6865

Usage Guidelines

- The status of MAC tunneling can be configured on a global or per-SVLAN basis.
  - When MAC tunneling is enabled globally, the per-SVLAN MAC tunneling configuration is not active.
  - When MAC tunneling is disabled globally, the per-SVLAN MAC tunneling configuration is active.
- Any changes to the global MAC tunneling status requires a switch reload to activate.
- The global tunnel MAC address is set to 01:00:0C:CD:CD:D0 by default, which is the CISCO tunnel MAC address that is used for Generic Bridge PDU Tunneling (GBPT). A different tunnel MAC address can also be configured for a specific UNI profile and will apply only to packets processed by that profile.
- When L2 protocol packets are received on a UNI port and the associated UNI profile for that port is configured with a MAC tunnel action for that protocol, the destination MAC address for the packets is changed to the tunnel MAC address. The packets are then sent out the NNI port associated with the SVLAN.
- When L2 tunneled packets (with a tunnel MAC as the destination address) are received on an NNI port, the tunnel MAC address is replaced with the protocol MAC address. The packets are then forwarded to the respective UNI port associated with the SVLAN.

Examples

```
-> ethernet-service mac-tunneling disable
INFO :Changed mac-tunnel feature status will take effect if command is saved on
next switch reboot
-> ethernet-service mac-tunneling enable
```

Release History

Release 8.6R1; command introduced.

Related Commands

ethernet-service svlan mac-tunneling	Configures the MAC tunneling status for an SVLAN.
show ethernet-service mac-tunneling	Displays the global status of MAC tunneling for the switch.

MIB Objects

```
alaEServiceGlobals
   alaEServiceGlobalMacTunneling
```

ethernet-service svlan mac-tunneling

Configures the MAC tunneling status on a per-SVLAN basis. Enabling MAC tunneling for specific SVLANs limits the trapping of GBPT packets for processing to only those SVLANs.

ethernet-service svlan *svid1***[-***svid2***] mac-tunneling {enable | disable}**

Syntax Definitions

*svlan_id***[-***svlan_id2***]**	The VLAN ID number identifying the SVLAN. Use a hyphen to specify a range of VLAN IDs (10-12).
enable	Enables the MAC tunneling status for the specified SVLAN.
disable	Disables the MAC tunneling status for the specified SVLAN.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6860, 6865

Usage Guidelines

- Enabling MAC tunneling on a per-SVLAN basis or on a global basis is mutually exclusive; make sure MAC tunneling is globally disabled before attempting to enable MAC tunneling for the specified SVLAN.
- When MAC tunneling is enabled globally, all GBPT packets are trapped for processing even if there is no MAC tunneling action configured for the associated UNI profile. This limits the rate at which these packets are forwarded.
- Enabling MAC tunneling for specific SVLANs limits the trapping of GBPT packets to only those SVLANs where it is needed for MAC tunneling; other SVLANs forward the traffic without trapping the GBPT packets.
- Use the **show ethernet-service vlan** command to display the MAC tunneling status for the SVLAN ID.
- A maximum of four SVLANs can have MAC tunneling enabled at the same time.

Examples

```
-> ethernet-service svlan 1000 mac-tunneling enable
-> ethernet-service svlan 2000-2005 mac-tunneling enable
-> ethernet-service svlan 1000 mac-tunneling disable

-> show ethernet-service vlan 2000
Name                    : VLAN 2000,
Type                    : Service Vlan,
Administrative State    : enabled,
```

```
Operational State        : disabled,
IP Router Port           : disabled,
IP MTU                   : 1500
MAC Tunneling            : enabled,
```

Release History

Release 8.6R1; command introduced.

Related Commands

ethernet-service mac-tunneling	Configures the global MAC tunneling status.
show ethernet-service vlan	Displays a list of VLANs and their attributes configured on the switch.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanMacTunneling
```

ethernet-service transparent-bridging

Configures transparent bridging which associates NNI ports with all VLANs even if they are not created on the switch.

ethernet-service transparent-bridging [nni port *chassis/slot/port***[-***port2***] | nni linkagg** *agg_id***[-***agg_id2***] {enable | disable}]**

Syntax Definitions

chassis	The chassis identifier.
slot/port **[-***port2***]**	The slot and port number.
*agg_id***[-***agg_id2***]**	The link aggregate ID.
enable	Enables the specified legacy BPDU support.
disable	Disables the specified legacy BPDU support.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Transparent bridging supports both global and port level enable/disable commands.
- Port level configuration is not accepted if transparent bridging is not enabled globally.
- If transparent bridging is disabled globally, all the port level transparent bridging configuration are deleted. The port level configuration must be re-configured after re-enabling transparent-bridging globally.
- Port level transparent bridging is allowed only when there is at least one SVLAN configure on NNI port.
- Transparent bridge is only supported on NNI ports.
- Transparent bridge can only be configured when STP is configured in flat mode.
- Transparent bridging cannot be configured when STP protocol mode set to MSTP.
- DHL and transparent bridging are not supported on the same NNI port.

Examples

```
-> ethernet-service transparent-bridging enable
-> ethernet-service nni port 1/1/5 transparent-bridging enable
-> ethernet-service nni linkagg 5 transparent-bridging enable
```

Release History

Release 8.3.1; command introduced.

Related Commands

show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortType
   alaEServicePortVendorTpid
   alaEServicePortLegacyStpBpdu
   alaEServicePortRowStatus
```

show ethernet-service vlan

Displays a list of VLANs configured on the switch. Use this command to identify VLAN Stacking SVLANs.

show ethernet-service vlan [*vlan_id***-[***vlan_id2***]]**

Syntax Definitions

vlan_id-**[***vlan_id2***]**	The VLAN ID number identifying the SVLAN. Use a hyphen to specify a range of VLAN IDs (10-12).

Defaults

By default, all VLANs are displayed if a VLAN or range of VLANs is not specified with this command.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

Specify a single VLAN ID or a range of VLAN IDs to display configuration information for the specific VLANs.

Examples

```
-> show ethernet-service vlan
 vlan    type   admin   oper    ip    mtu          name
------+-------+-------+------+------+------+------------------
1      std       Ena     Ena   Ena    1500    VLAN 1
200    std       Ena     Dis   Ena    1500    VLAN 200
300    std       Ena     Dis   Dis    1500    VLAN 300
400    router    Ena     Ena   Ena    1500    ROUTER VLAN 400
500    router    Ena     Dis   Ena    1500    ROUTER VLAN 500
777    std       Ena     Dis   Dis    1500    VLAN 777
800    vstk      Ena     Dis   Dis    1500    VLAN 800
1000   vstk      Ena     Dis   Dis    1500    VLAN 1000
1001   vstk      Ena     Dis   Dis    1500    VLAN 1001
1002   vstk      Ena     Dis   Dis    1500    VLAN 1002
1003   vstk      Ena     Dis   Dis    1500    VLAN 1003
1004   std       Ena     Dis   Dis    1500    VLAN 1004
1005   std       Ena     Dis   Dis    1500    VLAN 1005
1006   std       Ena     Dis   Dis    1500    VLAN 1006
1007   std       Ena     Dis   Dis    1500    VLAN 1007
1008   std       Ena     Dis   Dis    1500    VLAN 1008
1009   std       Ena     Dis   Dis    1500    VLAN 1009
1010   std       Ena     Dis   Dis    1500    VLAN 1010

-> show ethernet-service vlan 1000-1003
 vlan    type   admin   oper    ip    mtu          name
------+-------+-------+------+------+------+------------------
1000   vstk      Ena     Dis   Dis    1500    VLAN 1000
1001   vstk      Ena     Dis   Dis    1500    VLAN 1001
```

```
1002   vstk      Ena     Dis   Dis    1500    VLAN 1002
1003   vstk      Ena     Dis   Dis    1500    VLAN 1003
```

output definitions

vlan	The VLAN ID number identifying the instance.
type	The type of VLAN.
admin	The administrative state of the VLAN. (**Ena** or **Dis**).
oper	The operation status of the VLAN (**Ena** or **Dis**).
ip	The status of the IP router port (**Ena** or **Dis**).
mtu	The IP MTU value configured for the VLAN.
name	The user-defined text description for the VLAN. By default, the VLAN ID is specified for the description.

```
-> show ethernet-service vlan 1001
Name                     : VLAN 1001,
Type                     : Service Vlan,
Administrative State     : enabled,
Operational State        : disabled,
IP Router Port           : disabled,
IP MTU                   : 1500
MAC Tunneling            : disabled,
```

output definitions

Name	The user-defined text description for the VLAN. By default, the VLAN ID is specified for the description.
Type	The type of VLAN.
Administrative State	The administrative state of the VLAN (**enabled** or **disabled**).
Operational State	The operational status of the VLAN (**enabled** or **disabled**).
IP Router Port	The IP router interface status (**enabled** = IP router interface exists for the VLAN or **disabled** = no IP router port exists for the VLAN).
IP MTU	The IP MTU value configured for the VLAN.
MAC Tunneling	The MAC tunneling status for the VLAN (**enabled** or **disabled**).

Release History

Release 7.1.1; command introduced.
Release 8.6R1; “MAC Tunneling” field added.

Related Commands

ethernet-service svlan	Creates a VLAN Stacking VLAN (SVLAN) for tunneling customer traffic, a management SVLAN for provider traffic application uses to distribute multicast traffic.
ethernet-service svlan mac-tunneling	Configures the MAC tunneling status on a per-SVLAN basis.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanRouterStatus
   vlanType
   vlanMtu
   vlanMacTunneling
```

show ethernet-service

Displays configuration information for VLAN Stacking Ethernet services.

show ethernet-service [service-name *service_name* | **svlan** *svlan_id* | **transparent-bridging]**

Syntax Definitions

service_name	The name of an existing VLAN Stacking service. Use quotes around string if the service name contains multiple words with spaces between them (for example, “ALE Engineering”).
svlan_id	The VLAN ID number that identifies an existing SVLAN.

Defaults

By default, all services are displayed if a service name or SVLAN ID is not specified with this command.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Enter the name of a service to display configuration information for a specific service.
- Enter an SVLAN ID to display configuration information for all services that are associated with a specific SVLAN.

Examples

```
-> show ethernet-service

Service Name : VideoOne
    SVLAN   : 300
    NNI(s)  : 1/2/1, 1/2/2
    SAP Id  : 20
        UNIs        : 1/1/1, 1/1/2
        CVLAN(s)    : 10, 20
        sap-profile : sap-video1
    SAP Id  : 30
        UNIs        : 1/1/3
        CVLAN(s)    : untagged, 40
        sap-profile : sap-video2

Service Name : CustomerABC
    SVLAN   : 255
    NNI(s)  : 1/1/22
    SAP Id  : 10
        UNIs        : 1/2/1, 1/2/2
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile
```

```
-> show ethernet-service service-name CustomerABC

Service Name : CustomerABC
    SVLAN   : 255
    NNI(s)  : 1/1/22
    SAP Id  : 10
        UNIs        : 1/2/1, 1/2/2
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile

-> show ethernet-service svlan 300

Service Name : VideoOne
    SVLAN   : 300
    NNI(s)  : 1/2/1, 1/2/2
    SAP Id  : 20
        UNIs        : 1/1/1, 1/1/2
        CVLAN(s)    : 10, 20
        sap-profile : sap-video1
    SAP Id  : 30
        UNIs        : 1/1/3
        CVLAN(s)    : untagged, 40
        sap-profile : sap-video2

-> show ethernet-service transparent-bridging
Global Transparent Bridging               : enabled,
```

output definitions

Service Name	The name of the VLAN Stacking service.
SVLAN	Displays the SVLAN ID associated with the service. Note that SVLAN appears as the field name if the VLAN ID is an SVLAN.
NNI(s)	VLAN Stacking Network Network Interface ports associated with the service to tunnel SVLAN customer traffic.
SAP Id	The ID number for the VLAN Stacking Service Access Point that is applied to the service.
UNIs	VLAN Stacking User Network Interface ports that receive customer traffic.
CVLAN(s)	Customer VLAN IDs ingressing on UNI ports.
sap-profile	The name of the SAP profile associated with the SAP.
Global Transparent Bridging	Displays whether transparent bridging is enabled globally on the switch.

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service service-name	Creates a VLAN Stacking service and associates the service with an SVLAN.
ethernet-service transparent-bridging	Displays a list of all or a range of configured SVLANs or the parameters of a specified SVLAN.
ethernet-service transparent-bridging	Configures transparent bridging globally or on a port/linkagg.

MIB Objects

```
alaEServiceTable
   alaEServiceID
   alaEServiceSVLAN
alaEServiceNniSvlanTable
   alaEServiceNniSvlanNni
alaEServiceSapTable
   alaEServiceSapID
alaEServiceSapUniTable
   alaEServiceSapUniUni
alaEServiceSapCvlanTable
   alaEServiceSapCvlanCvlan
   alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
   alaEServiceProfileID
```

show ethernet-service sap

Displays configuration information for VLAN Stacking Service Access Points (SAP).

show ethernet-services sap [*sap_id***]**

Syntax Definitions

sap_id	The SAP ID number identifying the service instance.

Defaults

By default, all SAPs are displayed if a SAP ID is not specified with this command.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

Specify a single SAP ID to display configuration information for a specific SAP.

Examples

```
-> show ethernet-services sap

   SAP Id  : 10
        UNIs        : 1/2/1, 1/2/1
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile

    SAP Id  : 20
        UNIs        : 1/1/1, 1/1/2
        CVLAN(s)    : 10, 20
        sap-profile : sap-video1

    SAP Id  : 30
        UNIs        : 1/1/3
        CVLAN(s)    : 30, 40
        sap-profile : sap-video2

-> show ethernet-service sap 10

 SAP Id  : 10
        UNIs        : 1/2/1, 1/2/1
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile
```

output definitions

SAP Id	The ID number for the VLAN Stacking Service Access Point that is applied to the service.
UNIs	VLAN Stacking User Network Interface ports that receive customer traffic.

output definitions

CVLAN(s)	Customer VLAN IDs ingressing on UNI ports.
sap-profile	The name of the SAP profile associated with the SAP.

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service sap	Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking SAP profile and service.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.
show ethernet-service sap-profile	Displays the profile attribute configuration for SAP profiles.

MIB Objects

```
alaEServiceSapTable
   alaEServiceSapID
alaEServiceSapUniTable
   alaEServiceSapUniUni
alaEServiceSapCvlanTable
   alaEServiceSapCvlanCvlan
   alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
   alaEServiceProfileID7
```

show ethernet-service port

Displays configuration information for a VLAN Stacking service port.

show ethernet-service port {*chassis/slot/port* | **linkagg** *agg_id***}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
agg_id	The link aggregate ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

Specifying a slot/port or link aggregate ID number is required with this command.

Examples

```
-> show ethernet-service port 1/1/10

Interface : 1/1/10
Port Type   : UNI
    UNI Profile   : default-uni-profile
    Default SVLAN : 4095

Service Name : svlan_service
    SVLAN   : 20
    NNI(s)  : No NNIs configured
    SAP Id  : 1
        UNIs        : 1/1/10
        CVLAN(s)    : 200
        sap-profile : translate_profile

-> show ethernet-service port 1/1/22

Interface : 1/1/22
Port Type : NNI

Service Name : CustomerABC
    SVLAN   : 255
    NNI(s)  : 1/1/22
    SAP Id  : 10
        UNIs        : 1/2/1, 1/2/2
        CVLAN(s)    : 500, 600
        sap-profile : default-sap-profile
```

```
Service Name : Video-Service
    SVLAN   : 300
    NNI(s)  : 1/1/22, 1/2/3
    SAP Id  : 20
        UNIs        : 1/1/1, 1/1/2
        CVLAN(s)    : 10, 20
        sap-profile : sap-video1
    SAP Id  : 30
        UNIs        : 1/1/3
        CVLAN(s)    : 30, 40
        sap-profile : sap-video2
```

output definitions

Interface	The slot and port number or link aggregate ID for the specified interface.
Port Type	The type of VLAN Stacking port (**UNI** or **NNI**).
Service Name	The name of the VLAN Stacking service.
SVLAN	Displays the SVLAN ID associated with the service. Note that SVLAN appears as the field name if the VLAN ID is an SVLAN.
NNI(s)	VLAN Stacking Network Network Interface ports associated with the service to tunnel SVLAN customer traffic.
SAP Id	The ID number for the VLAN Stacking Service Access Point that is applied to the service.
UNIs	VLAN Stacking User Network Interface ports that receive customer traffic.
CVLAN(s)	Customer VLAN IDs ingressing on UNI ports.
sap-profile	The name of the SAP profile associated with the SAP.

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service svlan nni	Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN.
ethernet-service sap uni	Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking SAP.
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
alaEServiceTable
   alaEServiceID
   alaEServiceSVLAN
alaEServiceNniSvlanTable
   alaEServiceNniSvlanNni
alaEServiceSapTable
   alaEServiceSapID
alaEServiceSapUniTable
   alaEServiceSapUniUni
alaEServiceSapCvlanTable
   alaEServiceSapCvlanCvlan
   alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
   alaEServiceProfileID
```

show ethernet-service nni

Displays configuration information for VLAN Stacking Network Network Interface (NNI) ports.

show ethernet-service nni [port *chassis/slot/port* | **linkagg** *agg_id***]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
agg_id	The link aggregate ID number.

Defaults

By default, all NNI ports are displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

Specify a *slot/port* or link aggregate ID number to display information for a single slot/port or link aggregate ID.

Examples

```
-> show ethernet-service nni

  Port     TPID         Legacy BPDU           Transparent Bridging
                      stp         mvrp
--------+--------+----------------------+--------------------------
  1/1/22  0x8100    Disable     Disable             Enable
  1/1/23  0x8100    Disable     Disable             Enable

-> show ethernet-service nni 1/23

  Port     TPID         Legacy BPDU           Transparent Bridging
                      stp         mvrp
--------+--------+----------------------+--------------------------
  1/1/23  0x8100    Disable     Disable              Enable
```

output definitions

Port	The slot/port number or link aggregate ID for the NNI port.
TPID	The vendor TPID value configured for the NNI port.
stp	Whether Spanning Tree legacy BPDU processing is enabled for the NNI port.
mvrp	Whether MVRP legacy BPDU processing is enabled for the port.
Transparent Bridging	Whether transparent bridging is enabled or disabled.

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service svlan nni	Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN.
ethernet-service nni	Configures the vendor TPID value and the legacy BPDU processing status for a VLAN Stacking Network Network Interface (NNI).
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortVendorTpid
   alaEServicePortLegacyStpBpdu
   alaEServicePortLegacyGvrpBpdu
   alaEServicePortTransBridging
```

show ethernet-service nni l2pt-statistics

Displays statistics collected for Network Network Interface (NNI) ports.

show ethernet-services nni [port *chassis/slot/port* | **linkagg** *agg_id***] l2pt-statistics**

Syntax Definitions

chassis/slot/port	The chassis, slot, and port number (1/1/6).
agg_id	The link aggregate ID number (0–31).

Defaults

By default, statistics for all NNI ports are displayed.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the **port** *chassis/slot/port* or **linkagg** *agg_id* parameter to display statistics information for a specific switch port or link aggregate ID.
- Make sure the specified port or link aggregate is configured as an NNI port.

Examples

```
-> show ethernet-service nni l2pt-statistics
  Port   Rx Mac-Tunnel   Mac-tunnel discard
-------+---------------+--------------------
 1/1/23          1234             2
 1/1/24          256              0

-> show ethernet-service nni port 1/1/24 l2pt-statistics
  Port   Rx Mac-Tunnel   Mac-tunnel discard
-------+---------------+--------------------
 1/1/24          256              0

-> show ethernet-service nni port 1/1/5 l2pt-statistics
ERROR: Port (1/1/5) is not bound to any svlan
```

output definitions

Port	The chassis, slot, and port number or link aggregate ID for the NNI port.
Rx Mac-Tunnel	The total number of frames trapped to CPU with tunnel MAC.
Mac-tunnel discard	The total number of discarded frames that are trapped to CPU with tunnel MAC.

Release History

Release 8.6R2; command was introduced.

Related Commands

clear ethernet-service nni l2pt-statistics	Clears all NNI port statistics.
show ethernet-service nni	Displays configuration information for VLAN Stacking NNI ports.

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortType
alaEServiceNNIPortL2ProtocolStatisticsTable
   alaEServiceNNIPortL2RxMACTunneledFrames
   alaEServiceNNIPortL2MACTunneledDiscardFrames
```

clear ethernet-service nni l2pt-statistics

Clears statistics collected for Network Network Interface (NNI) ports.

clear ethernet-services nni [port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]] l2pt-statistics**

Syntax Definitions

*chassis/slot/port***[**-*port2***]**	The chassis, slot, and port number (1/1/6) on which to clear the statistics. Use a hyphen to specify a range of ports (1/1/6-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number on which to clear the statistics. Use a hyphen to specify a range of link aggregate IDs (5-10)

Defaults

By default, the statistics for all NNI ports are cleared if a port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the **port** *chassis/slot/port***[**-*port2***]** or **linkagg** *agg_id***[**-*agg_id2***]** parameter to clear statistics information for specific switch ports or link aggregate IDs.
- Make sure the specified port or link aggregate is configured as an NNI port.

Examples

```
-> clear ethernet-service nni l2pt-statistics
-> clear ethernet-service nni port 1/1/6 l2pt-statistics
-> clear ethernet-service nni port 1/1/7-10 l2pt-statistics
-> clear ethernet-service nni port 1/1/5 l2pt-statistics
ERROR: Port 1/1/5 is not a network port

-> clear ethernet-service nni linkagg 10 l2pt-statistics
-> clear ethernet-service nni linkagg 11-15 l2pt-statistics
-> clear ethernet-service nni linkagg 20 l2pt-statistics
ERROR: Port or Linkagg not Vlan Stacking Port
```

Release History

Release 8.6R2; command was introduced.

Related Commands

show ethernet-service nni l2pt-statistics	Displays the statistics information collected for NNI ports.

MIB Objects

```
alaEServiceL2PTProtocolStatisticsClear
   alaEServiceNNIPortL2GlobalClearStatistics
alaEServiceNNIPortL2ProtocolStatisticsTable
   alaEServiceNNIPortL2ClearStats
```

show ethernet-service uni

Displays a list of UNI ports configured for the switch and the profile association for each port.

show ethernet-service uni [port *chassis/slot/port* | **linkagg** *agg_id***]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
agg_id	The link aggregate ID number.

Defaults

By default, profile information for all UNI ports is displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

Specify a *chassis/slot/port* or link aggregate ID number to display information for a single port or link aggregate ID.

Examples

```
-> show ethernet-service uni

    Port    UNI Profile
---------+--------------------+
   1/1/1   uni-profile-default
   1/1/2   multi-site
   1/1/3   multi-site

-> show ethernet-service uni port 1/3

    Port    UNI Profile
---------+--------------------+
   1/1/3   multi-site
```

output definitions

Port	The chassis/slot/port number or link aggregate ID for the UNI port.
UNI Profile	The UNI profile associated with the port.

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service sap uni	Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking Service Access Point (SAP).
ethernet-service uni-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
show ethernet-service uni-profile	Displays the profile attribute configuration for VLAN Stacking UNI profiles.

MIB Objects

```
alaEServiceUniProfileTable
   alaEServicePortID
   alaEServicePortProfileID
```

show ethernet-service uni l2pt-statistics

Displays statistics collected for each tunneling protocol on a per-UNI port basis.

show ethernet-service uni [port *chassis/slot/port* | **linkagg** *agg_id***] l2pt-statistics**

Syntax Definitions

chassis/slot/port	The chassis, slot, and port number (3/1).
agg_id	The link aggregate ID number.

Defaults

By default, statistics information for all UNI ports and associated tunneling protocols is displayed.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the **port** *chassis/slot/port* or **linkagg** *agg_id* parameter to display statistics information for a specific switch port or link aggregate ID.
- Make sure the specified port or link aggregate is configured as a UNI port.

Examples

```
-> show ethernet-service uni L2PT-statistics
                                                    Mac          Source
 Port       L2 Protocol   Rx     Peer   Mac Tunnel De-tunnel      MAC
----------+------------+-------+-------+----------+----------+--------------
1/1/5       STP           10       0      10         10       000000:000001
1/1/5       802.1x        10       0      10         10       000000:000001
1/1/5       802.3ad       10      10       0          0       000000:000001
1/1/5       802.1ab        0       0       0          0       -
1/1/5       GVRP           0       0       0          0       -
1/1/5       AMAP           0       0       0          0       -
1/1/5       OAM            0       0       0          0       -
1/1/5       LACPMARKER     0       0       0          0       -
1/1/5       UDLD           0       0       0          0       -
1/1/5       PAGP           0       0       0          0       -
1/1/5       CDP            0       0       0          0       -
1/1/5       VTP           10       0      10         10       000000:000001
1/1/5       DTP           10       0      10         10       000000:000001
1/1/5       PVST           0       0       0          0       -
1/1/5       VLAN           0       0       0          0       -
1/1/5       UPLINK         0       0       0          0       -
1/1/5       MVRP           0       0       0          0       -

-> show ethernet-service uni port 1/1/4 l2pt-statistics
ERROR: Port (1/4) is not a user port
```

output definitions

Slot/Port	Service UNI port associated with an L2 protocol and L2 protocol statistics.
L2 Protocol	The l2 protocol associated with the service UNI port.
Rx	The total number of frames received by the protocol on the port and trapped in CPU.
Peer	The total number of tunneled frames received by the protocol on the port and trapped in CPU and peered.
Mac Tunnel	The total number of tunneled frames received by the protocol on the port and trapped in CPU and MAC tunneled.
Mac De-tunnel	The total number of tunneled frames received by the protocol on the port and trapped in CPU and MAC de-tunneled.
Source MAC	Specifies the source MAC address of the last frame of the protocol on the port trapped in CPU.

Release History

Release 8.6R2; command was introduced.

Related Commands

clear ethernet-service uni l2pt-statistics	Clears the tunneling protocol statistics on UNI ports.
show ethernet-service uni	Displays a list of UNI ports configured for the switch and the profile association for each port.

MIB Objects

```
alaEServicePortTable
   alaEServicePortID
   alaEServicePortType
alaEServiceUNIPortL2ProtocolStatisticsTable
   AlaEServiceUNIPortL2StatisticsEntry
   alaEServiceUNIPortL2ProtocolID
   alaEServiceUNIPortL2RxFrames
   alaEServiceUNIPortL2TunneledFrames
   alaEServiceUNIPortL2DroppedFrames
   alaEServiceUNIPortL2PeeredFrames
   alaEServiceUNIPortL2MACTunneledFrames
   alaEServiceUNIPortL2MACDeTunneledFrames
   alaEServiceUNIPortL2LastSourceMAC
```

clear ethernet-service uni l2pt-statistics

Clears tunneling protocol statistics collected for UNI ports.

clear ethernet-service uni [port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]] l2pt-statistics**

Syntax Definitions

*chassis/slot/port***[**-*port2***]**	The chassis, slot, and port number (1/1/6) on which to clear the statistics. Use a hyphen to specify a range of ports (1/1/6-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number on which to clear the statistics. Use a hyphen to specify a range of link aggregate IDs (5-10)

Defaults

By default, tunneling protocol statistics are cleared on all UNI ports if a port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the **port** *chassis/slot/port***[**-*port2***]** or **linkagg** *agg_id***[**-*agg_id2***]** parameter to clear statistics information for specific switch ports or link aggregate IDs.
- Make sure the specified port or link aggregate is configured as UNI port.

Examples

```
-> clear ethernet-service uni l2pt-statistics

-> clear ethernet-service uni port 1/1/1 12pt-statistics
-> clear ethernet-service uni port 1/1/7-10 l2pt-statistics
-> clear ethernet-service uni port 1/1/6 l2pt-statistics
ERROR: Port 1/1/6 is not a user port

-> clear ethernet-service uni linkagg 10 l2pt-statistics
-> clear ethernet-service uni linkagg 11-15 l2pt-statistics
-> clear ethernet-service uni linkagg 20 l2pt-statistics
ERROR: Port or Linkagg not Vlan Stacking Port
```

Release History

Release 8.6R2; command was introduced.

Related Commands

show ethernet-service uni l2pt-statistics	Displays tunneling protocol statistics on a per-UNI port.

MIB Objects

```
alaEServiceL2PTProtocolStatisticsClear
   alaEServiceNNIPortL2GlobalClearStatistics
alaEServiceUNIPortL2ProtocolStatisticsTable
   alaEServiceUNIPortL2ClearStats
```

show ethernet-service uni-profile

Displays the profile attribute configuration for VLAN Stacking User Network Interface (UNI) profiles.

show ethernet-service uni-profile [*uni_profile_name***]**

Syntax Definitions

uni_profile_name	An alphanumeric string. Use quotes around the string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

Defaults

By default, all UNI profiles are displayed if a UNI profile name is not specified with this command.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Specify a UNI profile name to display attributes for a single UNI profile.
- UNI profile information is displayed based on the switch platform. For example, UNI profile settings to process CISCO control packets and custom L2 protocol assignments for UNI profiles are supported only on the OmniSwitch 6465, OmniSwitch 6860, and OmniSwitch 6865, so that information is displayed only on those switches.

Examples

Sample output on an OmniSwitch 6465, OmniSwitch 6860, and OmniSwitch 6865:

```
-> show ethernet-service uni-profile
Profile Name: default-uni-profile
  Tunnel MAC : 01:00:0c:cd:cd:d0,
  STP : tunnel,     802.1x : drop,       802.3ad : peer,       802.1ab    : drop,
  MVRP: tunnel,     AMAP   : drop,       OAM     : peer,       LACPMARKER : peer,
  UDLD: peer,       PAGP   : drop,       CDP     : drop,       VTP        : drop,
  DTP : drop,       PVST   : drop,       VLAN    : drop,       UPLINK     : drop,
  802.1AB Tagged : drop,   802.1AB UnTagged: drop,       802.1AB Mode    : default
Profile Name: ieee-drop-all
  All IEEE Mac Addresses : 01:80:C2:00:00:00 - 01:80:C2:00:00:FF : drop
Profile Name: ieee-fwd-all
  All IEEE Mac Addresses : 01:80:C2:00:00:00 - 01:80:C2:00:00:FF : tunnel,
  Pause Frame               : 01:80:C2:00:00:01 : drop,
  Mac specific control frame : 01:80:C2:00:00:04 : drop
Profile Name: uni-prof1
  Tunnel MAC : 01:00:0c:cd:cd:d0,
  STP : tunnel,     802.1x : drop,       802.3ad : peer,       802.1ab    : drop,
  MVRP: tunnel,     AMAP   : drop,       OAM     : peer,       LACPMARKER : peer,
  UDLD: peer,       PAGP   : drop,       CDP     : drop,       VTP        : drop,
  DTP : drop,       PVST   : drop,       VLAN    : drop,       UPLINK     : drop
  802.1AB Tagged : drop,   802.1AB UnTagged: drop,       802.1AB Mode    : default
```

```
  tunnel-mac-ethertype                : mac-tunnel

  tunnel-mac-range                    : tunnel
```

output definitions

Profile Name	The name of the UNI profile.
Tunnel MAC	The MAC address used for MAC tunneling.
PROTOCOL: action	The protocol and configured action: **peer—**The UNI port is participating in the specified protocol. **drop—**Discards the specified PDU. **tunnel—**The PDU is tunneled across the provider network without modifying the MAC address. **mac-tunnel—**The PDU is tunneled across the provider network after changing the destination MAC address to the tunnel MAC address.
Custom L2 Protocol	The name of a custom L2 protocol that is assigned to the UNI profile. In the example output shown above, the “tunnel-mac-ethertype” and “tunnel-mac-range” custom L2 protocols are assigned to “uni-prof1”.

Sample output on an OmniSwitch 6900:

```
-> show ethernet-service uni-profile

                                                                  802.1AB 802.1AB 802.1AB
   Profile Name       Stp   802.1x 802.3ad  MVRP    AMAP    Both   Tagged  Untagged
------------------+-------+------+-------+-------+-------+-------+-------+--------
default-uni-profile  tunnel  drop   peer    tunnel  drop    drop     -       -
lldp-tag-untag       tunnel  drop   peer    tunnel  drop     -      tunnel  drop
uprofile-video1      tunnel  drop   peer    drop    tunnel  drop     -       -
```

output definitions

Profile Name	The name of the UNI profile.
PROTOCOL: action	The protocol and configured action: **peer—**The UNI port is participating in the specified protocol. **drop—**Discards the specified PDU. **tunnel—**The PDU is tunneled across the provider network without modifying the MAC address.

Release History

Release 7.1.1; command introduced.
Release 8.6R1; “Tunnel MAC” field added, additional protocol fields added to display action for CISCO PDUs, custom L2 protocol entry names and action included in display output.
Release 8.6R2; “802.1AB Both”, “802.1AB Tagged”, “802.1AB Untagged”, and “802.1AB Mode” fields added.

Related Commands

ethernet-service uni-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni-profile inbound 802.1ab	Configures the treatment of Layer 2 tagged and untagged 802.1AB control frames that are received on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
ethernet-service custom-L2-protocol	Creates a custom L2 protocol MAC address entry with an optional mask, EtherType, or SSAP/DSAP protocol identifier.
ethernet-service uni-profile custom-L2-protocol	Assigns a custom L2 protocol MAC address entry to a UNI profile.
show ethernet-service uni	Displays the profile associations for VLAN Stacking UNI ports.

MIB Objects

```
alaEServiceUNIProfileTable
   alaEServiceUNIProfileID
   alaEServiceUNIProfileStpBpduTreatment
   alaEServiceUNIProfile8021xTreatment
   alaEServiceUNIProfile8021ABTreatment
   alaEServiceUNIProfile8023adTreatment
   alaEServiceUNIProfileMvrpTreatment
   alaEServiceUNIProfileAmapTreatment
   alaEServiceUNIProfileVtpTreatment
   alaEServiceUNIProfileVlanTreatment
   alaEServiceUNIProfileUplinkTreatment
   alaEServiceUNIProfileUdldTreatment
   alaEServiceUNIProfilePvstTreatment
   alaEServiceUNIProfilePagpTreatment
   alaEServiceUNIProfileLacpmarkerTreatment
   alaEServiceUNIProfileDtpTreatment
   alaEServiceUNIProfileCdpTreatment
   alaEServiceUNIProfileTunnelMac
   alaEServiceUNIProfileIeeeMacTreatment
   alaEServiceUNIProfileOamTreatment
   alaEServiceUNIProfile8021ABTagTreatment
   alaEServiceUNIProfile8021ABUnTagTreatment
alaEServiceUNIProfileL2CustomProtocolTable
   alaEServiceUNIProfileL2CustomID
   alaEServiceUNIProfileL2CustomProtocolID
   alaEServiceUNIProfileL2CustomProtocolType
```

show ethernet-service custom-l2-protocol

Displays the custom L2 protocol configuration for the switch.

show ethernet-service custom-l2-profile [*custom_protocol_name***]**

Syntax Definitions

custom_protocol_name	The name of a configured custom L2 protocol entry.

Defaults

By default, all custom L2 protocol entries are displayed if a custom L2 protocol name is not specified with this command.

Platforms Supported

OmniSwitch 6465, 6860, 6865

Usage Guidelines

- Specify a custom L2 protocol name to display attributes for a specific custom protocol entry.
- A custom L2 protocol entry is assigned to a UNI profile. Use the **show ethernet-service uni-profile** command to display the custom L2 protocol entries assigned to a UNI profile.

Examples

```
-> show ethernet-service custom-l2-protocol
 Custom L2 Protocol            Mac                Mask        Ether-Type Sub-Type
                                                                  (or)      (or)
                                                               Ssap/Dsap    Pid
----------------------+------------------+-----------------+----------+----------
tunnel-mac-ethersubtype 01:80:c2:00:11:11       -             0x5556        120
tunnel-mac-ethertype    01:80:c2:00:11:11       -             0x5555         -
tunnel-mac-ssap/dsap    01:80:c2:00:11:11       -             0x43/0x43      3
tunnel-mac              01:80:c2:00:11:11       -                -           -
tunnel-mac-range        01:80:c2:00:11:11   ff:ff:ff:ff:ff:00    -           -
discard-mac-range       01:80:c2:00:11:11   ff:ff:ff:00:ff:ff    -           -

-> show ethernet-service custom-l2-protocol tunnel-mac-range
 Custom L2 Protocol            Mac                Mask        Ether-Type Sub-Type
                                                                  (or)      (or)
                                                               Ssap/Dsap    Pid
----------------------+------------------+-----------------+----------+----------
tunnel-mac-range        01:80:c2:00:11:11   ff:ff:ff:ff:ff:00    -           -
```

output definitions

Custom L2 Protocol	The name of the custom L2 protocol entry.
Mac	The multicast MAC address for the custom L2 protocol entry.
Mask	The MAC address mask to specify a range of MAC addresses.

output definitions

Ether-Type (or) Ssap/Dsap	The EtherType or SSAP/DSAP value for the MAC address entry.
Sub-Type (or) Pid	The optional Sub-Type value or the PID value for the MAC address entry. • A Sub-Type value is optionally entered when an EtherType value is specified. • A PID value is specified when an SSAP/DSAP value is specified.

Release History

Release 8.6R1; command introduced.

Related Commands

ethernet-service custom-L2-protocol	Creates a custom L2 protocol MAC address entry with an optional mask, EtherType, or SSAP/DSAP protocol identifier.
ethernet-service uni-profile custom-L2-protocol	Assigns a custom L2 protocol entry to a UNI profile.
show ethernet-service uni-profile	Displays the UNI profile configuration for the switch, which includes any custom L2 protocol assignments.

MIB Objects

```
alaEServiceCustomL2ProtocolTable
   alaEServiceCustomL2ProtocolName
   alaEServiceCustomL2ProtocolMac
   alaEServiceCustomL2ProtocolMask
   alaEServiceCustomL2ProtocolEtherType
   alaEServiceCustomL2ProtocolEtherSubType
   alaEServiceCustomL2ProtocolSsap
   alaEServiceCustomL2ProtocolDsap
   alaEServiceCustomL2ProtocolId
   alaEServiceCustomL2ProtocolRowStatus
```

show ethernet-service uni-profile l2pt-statistics

Displays the profile statistics collected for User Network Interface (UNI) profiles. Statistics are collected for all protocol frames (including custom L2 protocols) that are received on all ports that are bound to the UNI profile.

show ethernet-service uni-profile [*uni_profile_name***] l2pt-statistics**

Syntax Definitions

uni_profile_name	The name of the UNI profile.

Defaults

By default, statistics for all UNI profiles are displayed if a UNI profile name is not specified with this command.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

Specify a UNI profile name to display the statistics for a single UNI profile.

Examples

```
-> show ethernet-service uni-profile Profile-1 l2pt-statistics
UNI Profile: Profile-1
        Total RX:                                               0,
        L2 Protocol:
                STP
                        Rx:                                     0,
                        Hardware processing:                    FWD,
                GVRP, MVRP
                        Rx:                                     0,
                        Hardware processing:                    FWD,
                802.1ab
                        Rx:                                     0,
                        Hardware processing:                    DROP,
                AMAP
                        Rx:                                     0,
                        Hardware processing:                    DROP,
                802.3ad, OAM, LACPMARKER
                        Rx:                                     0,
                        Hardware processing:                    CPU,
                802_1x
                        Rx:                                     0,
                        Hardware processing:                    DROP,
                PAGP, UDLD, CDP, DTP, VTP, PVST, VLAN, UPLINK
                        Rx:                                     0,
                        Hardware processing:                    CPU,
                802.1ab Tagged
                        Rx:                                     0,
```

```
                Hardware processing:                    DROP,
        802.1ab Untagged
                Rx:                                     0,
                Hardware processing:                    DROP,
```

output definitions

UNI Profile	The UNI profile associated with the port.
Total RX	The total number of protocol frames received on the port that is associated with the UNI profile.
L2 Protocol:	The protocol for which the statistics are collected.
Rx:	The number of frames received for the specific protocol.
Hardware processing:	Displays the configured hardware action.

Release History

Release 8.6R2; command was introduced.

Related Commands

clear ethernet-service uni-profile l2pt-statistics	Clears the statistics for all UNI profiles.
ethernet-service uni-profile	Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
ethernet-service uni uni-profile	Associates a VLAN Stacking UNI profile with a UNI port.
show ethernet-service uni	Displays the profile associations for VLAN Stacking UNI ports.
show ethernet-service uni l2pt-statistics	Displays tunneling protocol statistics for UNI ports.

MIB Objects

```
alaEServiceUNIProfileL2ProtocolTotalStatisticsTable
   alaEServiceUNIProfile
   alaEServiceUNIProfileL2ProtocolTotalRxFrames
alaEServiceUNIProfileL2ProtocolStatisticsTable
   alaEServiceUNIProfileID
   alaEServiceUNIProfileL2ProtocolIndex
   alaEServiceUNIProfileL2ProtocolRxFrames
   alaEServiceUNIProfileL2ProtocolTreatment
alaEServiceUNIProfileCustomL2ProtocolStatisticsTable
   alaEServiceUNIProfileCustomL2StatsProfileID
   alaEServiceUNIProfileCustomL2ProtocolIndex
   alaEServiceUNIProfileCustomL2ProtocolRxFrames
   alaEServiceUNIProfileCustomL2ProtocolTreatment
```

clear ethernet-service uni-profile l2pt-statistics

Clears the protocol statistics collected for UNI profiles.

clear ethernet-service uni-profile [*uni_profile_name***] l2pt-statistics**

Syntax Definitions

uni_profile_name	The name of the UNI profile.

Defaults

By default, statistics are cleared for all UNI profiles.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

Specify a UNI profile name to clear the statistics for a single UNI profile.

Examples

```
-> clear ethernet-service uni-profile uni-profile 1 l2pt-statistics
```

Release History

Release 8.6R2; command was introduced.

Related Commands

show ethernet-service uni-profile l2pt-statistics	Displays the statistics of all protocols configured per UNI port.

MIB Objects

```
alaEServiceL2PTProtocolStatisticsClear
   alaEServiceUNIProfileL2GlobalClearStatistics
alaEServiceUNIProfileL2ProtocolTotalStatisticsTable
   alaEServiceUNIProfile
   alaEServiceUNIProfileL2ProtocolClearStats
```

show ethernet-service mac-tunneling

Displays the global MAC tunneling status for the switch.

show ethernet-service mac-tunneling

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865

Usage Guidelines

Any changes to the global MAC tunneling status requires a switch reload to activate.

Examples

```
-> show ethernet-service mac-tunneling
Mac-Tunneling Feature: enable

-> ethernet-service mac-tunneling disable
INFO :Changed mac-tunnel feature status will take effect if command is saved on
next switch reboot

-> show ethernet-service mac-tunneling
(*=new mac-tunneling feature will be applied after reboot)
Mac-Tunneling Feature: disable*
```

Release History

Release 8.6R1; command introduced.

Related Commands

ethernet-service mac-tunneling Configures the global MAC tunneling status for the switch

MIB Objects

```
alaEServiceGlobals
   alaEServiceGlobalMacTunneling
```

show ethernet-service sap-profile

Displays the profile attribute configuration for VLAN Stacking Service Access Point (SAP) profiles.

show ethernet-service sap-profile *sap_profile_name*

Syntax Definitions

uni-profile-name	An alphanumeric string. Use quotes around the string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

Defaults

By default, all SAP profiles are displayed if a SAP profile name is not specified with this command.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900

Usage Guidelines

- Specify a SAP profile name to display attributes for a single SAP profile.
- The ingress bandwidth value is displayed in megabytes.

Examples

```
-> show ethernet-service sap-profile

      Profile Name   Ingr/Egr     Ingr Bw    Inner Tag   Priority   Priority
                        Bw        Sharing      Option    Mapping     Value
-------------------+-----------+-----------+-----------+----------+-----------
default-sap-profile     0/0       Enable      Preserve     fixed       0
map_pbit                0/0       Enable      Preserve     in-out      P
sap1                 24324/0      NA          Preserve     NA          NA
sap_1                   0/0       NA          Preserve     NA          NA

-> show ethernet-service sap-profile sap-video1

   Profile Name       Ingr/Egr    Ingr Bw       Inner Tag  Priority   Priority
                       Bw         Sharing       Option     Mapping     Value
-------------------+----------+-------------+-----------+----------+------------
sap-video1              20         Disable     Preserve     NA          NA
```

output definitions

Profile Name	The name of the SAP profile.
Ingr/Egr Bw	**Ingress Egress Bandwidth** - The maximum amount of ingress and egress bandwidth to allow for SAP ports.

output definitions

Ingr Bw Sharing	**Ingress Bandwidth Sharing -** The status of bandwidth sharing (**enable**, **disable,** or **NA**). If enabled, the ingress bandwidth value is shared across all SAP ports and CVLANs. If disabled, the bandwidth value is not shared and applied to individual SAP ports and CVLANs.
Inner Tag Option	Indicates how the CVLAN tag is processed (**translate** or **preserve**). If set to **preserve**, the CVLAN tag is retained and the SVLAN is added to the frame. If set to **translate**, the CVLAN tag is changed to the SVLAN tag.
Priority Mapping	Indicates how the priority value is configured for the SVLAN (**NA**, **in-out** or **fixed**). If set to **in-out**, the CVLAN priority value is mapped to the SVLAN. If set to fixed, a user-specified priority value is used for the SVLAN priority.
Priority Value	Indicates the priority value mapped to the SVLAN (**NA**, default 0, a number, **P**, or **DSCP**). A number indicates a fixed, user-specified value is used; **P** indicates the CVLAN 802.1p bit value is used; **DSCP** indicates the CVLAN DSCP value is used.

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service sap-profile	Creates a profile for a VLAN Stacking Service Access Point (SAP).
ethernet-service sap	Creates a VLAN Stacking SAP and associates the SAP with a service and SAP profile.
ethernet-service sap sap-profile	Specifies a different SAP profile for the SAP.
show ethernet-service sap	Displays configuration information for VLAN Stacking SAPs.

MIB Objects

```
alaEServiceSapProfileTable
   alaEServiceSapProfileID
   alaEServiceSapProfileCVLANTreatment
   alaEServiceSapProfilePriorityMapMode
   alaEServiceSapProfileFixedPriority
   alaEServiceSapProfileIngressBW
   alaEServiceSapProfileEgressBW
   alaEServiceSapProfileBandwidthShare
```

loopback-test

Configures a wire-rate hardware loopback test profile and enables or disables the activation of the profile. The loopback test profile specifies the switch attributes that are required to conduct an ingress or egress loopback operation on a switch port.

loopback-test *profile_name* **destination-mac** *dest_address* {**port** *chassis/slot/port* **| linkagg** *agg_id*} **source-mac** *src_address* **vlan** *vlan_id* **[type {inward | outward [sap** *sap_id*]**}]**

loopback-test *profile_name* **admin-state {enable | disable}**

no loopback-test *profile_name*

Syntax Definitions

profile_name	Alphanumeric string of up to 31 characters. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “Alcatel-Lucent Engineering”).
src_address	A unique source MAC address for the test frame.
dest_address	A unique destination MAC address for the test frame.
vlan_id	The VLAN ID of the test frame. Always use the outer VLAN ID.
chassis/slot/port	The switch port number to use for the loopback test.
agg_id	The linkagg ID for the loopback test. *This is currently not supported.*
inward	Sets the type of loopback test to ingress.
outward	Sets the type of loopback test to egress.
sap_id	UNI profile used for egress UNI loopback. *This is currently not supported.*
enable	Enables the loopback test profile.
disable	Disables the loopback test profile.

Defaults

parameter	default
type	**inward**

Platforms Supported

OmniSwitch 6860, 6865, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- Use the **no** form of this command to delete a loopback profile.
- Use the **loopback-test admin-state enable** command to enable the loopback test profile on the specified port. When the profile is enabled, the loopback operation is enabled for the port.
- Use the **loopback-test admin-state disable** command to disable the loopback operation for the specified port.

- 'loopback-test <*profile-name*> admin-state enable' command will not be displayed in 'show configuration snapshot'. Similarly, 'loopback-test admin-state <*profile-name*> enable' is not stored in vcboot.cfg.
- When a port is configured as outward loopback port, it goes "out-of-service" and will no longer carry customer traffic but remains active for test frame traffic. However, an inward loopback port remains "in-service" and will continue to carry customer traffic as well as test frame traffic.
- Only Layer 2 loopback tests are supported, so test frames are not routed. As a result, the loopback test operation will only swap the source and destination MAC address of bridged test frames.
- Test frame must be L3 frames and L3 header must be included in test frames.
- Traffic with all the valid CVLANS, which are part of the SVLAN gets looped-back, as hardware loopback cannot identify which CVLAN traffic to loopback.
- During outward loopback test, port will enter MAC-loopback, STP and Source Learning will be disabled on that port.
- In outward UNI/NNI loopback, destination MAC is learned as static MAC on loopback port on **loopback-test enable** and is removed on **loopback-test disable**. This destination MAC is not displayed in 'show mac-learning' command.
- The destination MAC address for the test frame must be unique to the network and must not be used anywhere in the device.

Examples

The following example creates an ingress loopback test profile:

```
-> loopback-test PE1-inward-UNI destination-mac 00:00:00:cc:aa:bb port 1/1/2
source-mac 00:00:00:dd:aa:01 vlan 1001 type inward
```

The following example creates an egress loopback test profile:

```
-> loopback-test PE2-outward-UNI destination-mac 00:00:00:cc:ab:bb port 1/1/2
source-mac 00:00:00:dd:ab:01 vlan 1001 type outward
```

The following command examples enable and disable a loopback test profile:

```
-> loopback-test PE1-outward-UNI admin-state enable
-> loopback-test PE1-outward-UNI admin-state disable
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show loopback-test	Displays the profile configuration for a loopback test profile.

MIB Objects

```
alaTestHwLoopbackProfileTable
   alaTestHwLoopbackProfileName
   alaTestHwLoopbackSourceMac
   alaTestHwLoopbackDestinationMac
   alaTestHwLoopbackVlan
   alaTestHwLoopbackPort
   alaTestHwLoopbackType
   alaTestHwLoopbackSapId
   alaTestHwLoopbackPortPktCounter
   alaTestHwLoopbackPortByteCounter
   alaTestHwLoopbackProfileStatus
   alaTestHwLoopbackProfileRowStatus
```

show loopback-test

Displays the profile configuration for a hardware loopback test profile.

show loopback-test [*profile_name***]** [**counters**]

Syntax Definitions

profile_name	The name of an existing hardware loopback test profile.
counters	Hardware counters for given or all loopback test profiles.

Defaults

By default, all profiles are displayed if a profile name is not specified with this command.

Platforms Supported

OmniSwitch 6860, 6865, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- Use the *profile_name* parameter to display the loopback test configuration for a specific profile.
- Hardware counters is displayed only when the test profile is enabled.

Examples

```
-> show loopback-test
Profile-Name         Src-Mac              Dest-Mac        Vlan    Port     Type    Status
-----------------+-----------------+-----------------+------+--------+--------+--------
test3              00:00:00:00:00:04  00:00:00:00:00:03  1000     1/1/11  Outward  Disable
test1              00:00:00:00:00:05  00:00:00:00:00:04  1000     1/1/11  Outward  Enable
test2              00:00:00:00:00:05  00:00:00:00:00:04  1000     1/1/11  Outward  Disable
test4              00:00:00:00:00:05  00:00:00:00:00:04  1000     1/1/11  Outward  Disable
test5              00:00:00:00:00:05  00:00:00:00:00:04  1000     1/1/11  Outward  Disable
test6              00:00:00:00:00:05  00:00:00:00:00:04  1000     1/1/11  Outward  Disable
test7              00:00:00:00:00:05  00:00:00:00:00:04  1000     1/1/11  Outward  Disable
profile2           00:aa:aa:aa:aa:dd  00:bb:bb:bb:bb:cc  100      1/1/20  Outward  Config
Total Entries = 8

-> show loopback-test counters
Profile-Name      Port     Type      Status    Packet Counters     Byte Counters
---------------+-------+--------+-----------+-----------------+-----------------
test3             1/1/11  Outward   Disable      69507476          34753738004
test1             1/1/11  Outward   Enable       1267025494        633512760908
test2             1/1/11  Outward   Disable      0                 0
```

output definitions

Profile-Name	The name of the loopback test profile.
Src-Mac	The source MAC address of the test packet.
Dest-Mac	The destination MAC address of the test packet.
Vlan	The VLAN ID of the loopback port.
Port	The UNI or NNI loopback port.

output definitions

Type	The type of loopback test; **Inward** (ingress) or **Outward** (egress).
Status	The status of the loopback test (**Enable**, **Disable**, or **Config**).
Packet Counters	Hardware packet counters for the configured flow.
Byte Counters	Hardware byte counters for the configured flow.

Release History

Release 8.6R1; command was introduced.

Related Commands

loopback-test	Configures a wire-speed Ethernet loopback test profile and enables or disables the activation of the profile.

MIB Objects

N/A

clear loopback-test counters

Clears the hardware counters of all the loopback test profiles.

clear loopback-test counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

N/A

Examples

```
-> clear loopback-test counters
```

Release History

Release 8.6R1; command was introduced.

Related Commands

loopback-test	Configures a wire-speed Ethernet loopback test profile and enables or disables the activation of the profile.

MIB Objects

N/A

8 Distributed Spanning Tree Commands

The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the OmniSwitch STP implementation distributes the Spanning Tree load between the primary management module and the network interface modules. This functionality improves network robustness by providing a Spanning Tree that continues to respond to BPDUs and port link up and down states in the event of a fail over to a backup management module or switch.

In addition to a distributed architecture, this implementation also provides the following Spanning Tree features:

- Automatic configuration of a physical topology into a single Spanning Tree to ensure that there is only one data path between any two switches.
- Fault tolerance within the network topology. The Spanning Tree is reconfigured in the event of a data path or bridge failure or when a new switch is added to the topology.
- Support for four Spanning Tree protocols: 802.1D (STP), 802.1W (RSTP), and 802.1Q 2005 (MSTP).
- A *flat* Spanning Tree operating mode. If STP or RSTP is used, this mode applies a single STP instance across all VLANs. If MSTP is used, this mode applies a single STP instance to each Multiple Spanning Tree Instance (MSTI), which identifies a set of VLANs.
- A *per-VLAN* Spanning Tree operating mode that applies a single STP instance for each defined VLAN on the switch.
- An STP topology that includes 802.1Q tagged ports and link aggregate logical ports in the calculation of the physical topology.

MIB information for Distributed Spanning Tree commands is as follows:

Filename: ALCATEL-IND1-VLAN-STP-MIB.mib
Module: alcatelIND1VLANSTPMIB

A summary of the available commands is listed here:

Bridge commands	**spantree mode** **spantree protocol** **spantree priority** **spantree hello-time** **spantree max-age** **spantree forward-delay** **spantree bpdu-switching** **spantree path-cost-mode** **spantree vlan admin-state** **spantree auto-vlan-containment** **show spantree** **show spantree cist** **show spantree msti** **show spantree vlan** **show spantree mode**
Port commands	**spantree cist** **spantree vlan** **spantree priority** **spantree cist path-cost** **spantree msti path-cost** **spantree vlan path-cost** **spantree cist mode** **spantree loop-guard** **spantree vlan mode** **spantree cist connection** **spantree vlan connection** **spantree cist admin-edge** **spantree vlan admin-edge** **spantree cist auto-edge** **spantree vlan auto-edge** **spantree cist restricted-role** **spantree vlan restricted-role** **spantree cist restricted-tcn** **spantree vlan restricted-tcn** **spantree cist txholdcount** **spantree vlan txholdcount** **show spantree ports** **show spantree cist ports** **show spantree msti ports** **show spantree vlan ports**
MST region commands	**spantree mst region name** **spantree mst region revision-level** **spantree mst region max-hops** **show spantree mst**
MST instance commands	**spantree msti** **spantree msti vlan** **show spantree msti vlan-map** **show spantree cist vlan-map** **show spantree map-msti**
PVST+ commands	**spantree pvst+compatibility**

spantree mode

Selects the flat Spanning Tree or per-VLAN Spanning Tree operating mode for the switch. These modes are exclusive; however, it is not necessary to reboot the switch when the STP modes are changed.

spantree mode {**flat | per-vlan}**

Syntax Definitions

flat	One Spanning Tree instance per switch.
per-vlan	One Spanning Tree instance for each VLAN configured on a switch.

Defaults

By default, the Spanning Tree mode for the switch is set to per-VLAN.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The Multiple Spanning Tree Protocol (MSTP), as defined in the IEEE 802.1Q 2005 standard, is only supported on switches operating in the flat Spanning Tree mode.
- If standard STP or RSTP is used when the switch is running in the flat mode, a single STP instance is applied across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 connect to the same switch together, then STP blocks one of these ports.
- If MSTP is used when the switch is running in the flat mode, a single STP instance is applied to each Multiple Spanning Tree Instance (MSTI). Each MSTI represents a set of VLANs.
- Flat Spanning Tree mode supports fixed (untagged) and 802.1Q tagged ports in each VLAN. However, Bridge Protocol Data Units (BPDUs) are always untagged.
- If the per-VLAN mode is selected, a single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances. In essence, a VLAN is a virtual bridge that has its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max-age, and forward delay.
- When operating in per-VLAN mode, 802.1Q tagged ports participate in an 802.1Q Spanning Tree instance that allows the Spanning Tree to extend across tagged VLANs. As a result, a tagged port can participate in more than one Spanning Tree instance; one for each VLAN that the port carries.
- If a VLAN contains both fixed and tagged ports and the switch is operating in per-VLAN Spanning Tree mode, then a hybrid of the two Spanning Tree instances (single and 802.1Q) is applied. If a VLAN appears as a tag on a port, then the BPDU for that VLAN are also tagged. However, if a VLAN appears as the configured default VLAN for the port, then BPDU are not tagged and the single Spanning Tree instance applies.
- Regardless of which mode the switch is running in, it is possible to administratively disable the Spanning Tree status for an individual VLAN (see Chapter 5, “VLAN Management Commands”).

Note. Active ports associated with such a VLAN are excluded from any Spanning Tree calculations and remain in a forwarding state.

Examples

```
-> spantree mode flat
-> spantree mode per-vlan
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree protocol	Selects the Spanning Tree protocol for the specified instance.
spantree bpdu-switching	Enables the switching of Spanning Tree BPDU on a VLAN that has Spanning Tree disabled.
show spantree	Displays VLAN Spanning Tree parameter values.

MIB Objects

```
vStpTable
   vStpNumber
   vStpMode
```

spantree protocol

Configures the Spanning Tree protocol for the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance.

spantree [cist | vlan *vlan_id***] protocol {stp | rstp | mstp}**

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
vlan_id	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
stp	IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
rstp	IEEE 802.1W Rapid Spanning Tree Protocol.
mstp	IEEE 802.1Q 2005 Multiple Spanning Tree Protocol. This protocol is not supported on a per-VLAN basis.

Defaults

By default, the Spanning Tree protocol is set to RSTP.

parameter	default
cist | vlan *vlan_id*	**cist**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the optional **cist** or **vlan** parameter is not specified with this command, the protocol is set for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active.

Note. Selecting MSTP is only an option for the flat mode CIST instance and is required to configure Multiple Spanning Tree Instances (MSTI).

- MSTP is only active when the switch is operating in the flat Spanning Tree mode. STP and RSTP are active when the switch is operating in either the flat or per-VLAN Spanning Tree mode.
- Deleting all existing MSTIs is required before changing the protocol from MSTP to STP or RSTP.

Note. When the protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values. However, if the path cost mode was set to 32-bit prior to the protocol change, the path cost is *not* reset to the default value. See the **spantree path-cost-mode** command page for more information.

Examples

```
-> spantree protocol mstp
-> spantree cist protocol mstp
-> spantree vlan 5 protocol rstp
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsProtocolSpecification
```

spantree vlan admin-state

Enables or disables the Spanning Tree status for a VLAN.

spantree vlan *vlan_id* **[**-*vlan_id2***] admin-state {enable | disable}**

Syntax Definitions

*vlan_id***[**-*vlan_id2***]**	An existing VLAN ID number. Use a hyphen to specify a range of VLANs (10-15).
enable	Enables Spanning Tree for the specified VLAN.
disable	Disables Spanning Tree for the specified VLAN.

Defaults

By default, the Spanning tree status is enabled for a VLAN instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

VLAN Spanning Tree instances are only active when the switch is running in the per-VLAN mode. However, configuring the VLAN Spanning Tree status is allowed in both modes (per-VLAN and flat).

Examples

```
-> spantree vlan 850-900 admin-state enable
-> spantree vlan 720-750 admin-state disable
-> spantree vlan 500 admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan	Creates a VLAN.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanAdmStatus
   vlanOperStatus
   vlanStatus
```

spantree mst region name

Defines the name for a Multiple Spanning Tree (MST) region. One of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 2005 standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

spantree mst region name *name*

no spantree mst region name

Syntax Definitions

name	An alphanumeric string. Use quotes around string if the name contains multiple words with spaces between them (for example, “ALE Marketing”).

Defaults

By default, the MST region name is left blank.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the MST region name.

Note. It is not necessary to specify the region name to remove it.

- To change the existing region, use this command with a string value that is different than the existing region name.
- Specifying an MST region name is allowed regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values, such as region name, only apply when the switch is operating in the flat Spanning Tree mode and using MSTP.

Examples

```
-> spantree mst region name SalesRegion
-> spantree mst region name “ALE Marketing”
-> no spantree mst region name
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region revision-level	Defines the revision level for an MST region.
spantree mst region max-hops	Defines the maximum number of hops for the MST region.
spantree msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
spantree msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigName
```

spantree mst region revision-level

Defines the revision level for a Multiple Spanning Tree (MST) region. One of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 2005 standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

spantree mst region revision-level *rev_level*

Syntax Definitions

rev_level	A numeric value that identifies the MST region revision level for the switch.

Defaults

By default, the MST revision level is set to zero.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

An MST region revision level can be assigned to the MST region regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values, such as revision level, only apply when the switch is operating in the flat Spanning Tree mode, using the MSTP.

Examples

```
-> spantree mst region revision-level 1000
-> spantree mst region revision-level 2000
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region name	Defines the name for an MST region.
spantree mst region max-hops	Defines the maximum number of hops for the MST region.
spantree msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
spantree msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigRevisionLevel
```

spantree mst region max-hops

Configures the maximum number of hops that are authorized to receive Multiple Spanning Tree (MST) regional information. Use this command to assign the maximum number of hops a BPDU is allowed to traverse, before it is discarded and related information is aged out.

spantree mst region max-hops *max_hops*

Syntax Definitions

max_hops	A numeric value that designates the maximum number of hops.

Defaults

By default, the maximum number of hops is set to 20.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The value configured with this command is a regional value that applies to all instances and is used to determine the size of the region.
- The maximum hop count value is the initial value of the “remaining hops” parameter in the MST BPDU that originates from the bridge that is serving as the root bridge for the region. Each bridge that in turn receives the MST BPDU decrements the “remaining hops” count value by one and passes the new value along to the next bridge. When the count reaches 0, the BPDU is discarded.
- Specifying an MST maximum hop count is allowed regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values only apply when the switch is operating in the flat Spanning Tree mode and using the MSTP.

Examples

```
-> spantree mst region max-hops 40
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region name	Defines the name for an MST region.
spantree mst region revision-level	Defines the revision level for an MST region.
spantree msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
spantree msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionMaxHops
```

spantree msti

Defines a Multiple Spanning Tree Instance (MSTI) number. This number identifies an association between a range of VLANs and a single Spanning Tree instance. In addition, it is possible to assign an optional name to the MSTI for further identification.

spantree msti *msti_id* **[name** *name***]**

no spantree msti *msti_id* **[name]**

Syntax Definitions

msti_id	A numeric MSTI ID number. A range of VLANs is associated to an MSTI ID number.
name	An alphanumeric string. Use quotes around string if the name contains multiple words with spaces between them (for example, “ALE Marketing”).

Defaults

By default, a flat mode Common and Internal Spanning Tree (CIST) instance always exists. The MSTI ID number for this instance is 0.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the MSTI from the switch configuration.
- Use the **no** form of this command along with the **name** parameter to remove the optional MSTI name from the specified instance. The instance itself is not removed; only the name.
- There is always one CIST per switch. Initially all VLANs are associated with the CIST instance.
- Creating an MSTI is allowed when the switch is operating in either the per-VLAN or flat Spanning Tree mode, as long as MSTP is the selected flat mode protocol. The MSTI configuration, however, is not active unless the switch is running in the flat mode.

Examples

```
-> spantree msti 10
-> spantree msti 20 name BldgOneST10
-> no spantree msti 20 name
-> no spantree msti 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region name	Defines the name for an MST region.
spantree mst region revision-level	Defines the revision level for an MST region.
spantree mst region max-hops	Defines the maximum number of hops for the MST region.
spantree msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapAddition
   vStpMstInstanceVlanBitmapDeletion
   vStpMstInstanceVlanBitmapState
```

spantree msti vlan

Defines an association between a range of VLANs and a single Multiple Spanning Tree Instance (MSTI). The MSTI-to-VLAN mapping created with this command is one of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 2005 standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

spantree msti *msti_id* **vlan** *vlan_id***[-***vlan_id2***]**

no spantree msti *msti_id* **vlan** *vlan_id***[-***vlan_id2***]**

Syntax Definitions

msti_id	A numeric MSTI identification number. A range of VLANs are associated to an MSTI ID number.
*vlan_id***[-***vlan_id2***]**	A VLAN ID number. Use a hyphen to specify a range of VLAND IDs (for example, **vlan 10-15**).

Defaults

By default, all VLANs are associated with the flat mode Common and Internal Spanning Tree (CIST) instance, which is also known as MSTI 0.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a VLAN or a range of VLANs from the specified MSTI association.
- Note that the VLAN ID specified with this command does not have to already exist in the switch configuration. This command maps VLAN IDs to MSTIs, but does not create VLANs.
- A VLAN is associated with only one MSTI at a time, but it is possible to move a VLAN from one MSTI to another. In addition, it is also possible to assign only one VLAN to an MSTI; a range of VLANs is not required.
- To associate multiple VLANS in a single command, use a hyphen to specify a range of VLAN IDs and a space to separate multiple VLAN IDs and/or ranges (for example 100-115 122 135 200-210).
- Configuring an MSTI-to-VLAN mapping is allowed when the switch is operating in either the per-VLAN or flat Spanning Tree mode, as long as MSTP is the selected flat mode protocol. The MSTI configuration, however, is not active unless the switch is running in the flat mode.

Examples

```
-> spantree msti 10 vlan 100-115
-> spantree msti 20 vlan 122
-> no spantree msti 10 vlan 100-115
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region name	Defines the name for an MST region.
spantree mst region revision-level	Defines the revision level for an MST region.
spantree mst region max-hops	Defines the maximum number of hops for the MST region.
spantree msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.

MIB Objects

```
vStpMstVlanAssignmentTable
   vStpMstVlanAssignmentVlanNumber
   vStpMstVlanAssignmentEntry
   vStpMstVlanAssignmentMstiNumber
```

spantree priority

Configures the bridge priority value for the Common and Internal Spanning Tree (CIST) instance, a Multiple Spanning Tree Instance (MSTI), or a VLAN instance. This command is also used to configure the priority value for a port or link aggregate associated with the CIST, an MSTI, or a VLAN.

spantree [cist | msti *msti_id* **| vlan** *vlan_id***] [port** *chassis/slot/port***[-***port2***]** | **linkagg** *agg_id***[-***agg_id2***]] priority** *priority*

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
msti_id	An existing MSTI ID number. If MSTI 0 is specified, the priority applies to the CIST instance. This parameter is configurable in both modes (flat or per-VLAN) but only if the flat mode protocol is set to MSTP.
vlan_id	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
priority	A bridge or port priority value. The valid range for the bridge priority is 0–65535. The valid range for the port priority is 0–15. If MSTP is the active flat mode protocol, enter a value that is a multiple of 4096 (for example, 4096, 8192, 12288).

Defaults

- By default, the bridge priority value is set to 32768 for the CIST, an MSTI, and a VLAN instance.
- By default, the port or link aggregate priority value is set to 7.

parameter	default
cist | **msti** *msti_id* | **vlan** *vlan_id*	**cist**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The bridge priority is used to determine which bridge the Spanning Tree algorithm designates as the root bridge. The port priority value is used to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

- The lower the bridge or port priority number assigned, the higher the priority that is associated with the bridge or port.
- If none of the optional instance parameters (**cist**, **msti**, or **vlan**) or **port** and **linkagg** parameters are specified with this command, the bridge priority is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the **cist**, **msti**, and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified priority values are not applied unless the supporting mode (flat for CIST/MSTI or per-VLAN for a VLAN instance) is active.
- To configure the bridge priority with this command, specify the instance (**cist**, **msti**, or **vlan**) and the priority value; do not specify a port number or link aggregate ID.
- The bridge priority value for an MSTI is calculated by adding the configured priority value to the Spanning Tree instance number. For example, if the priority value of MSTI 10 equals 32768 (the default), then the Spanning Tree priority value advertised for this instance is 32770 (32768 + 10).
- When the protocol is changed to/from MSTP, the bridge priority for the flat mode CIST instance is reset to the default value.
- The bridge priority specifies the priority value for the first two octets of the Bridge ID (eight octets long). The remaining six octets of the Bridge ID contain a dedicated bridge MAC address. In regards to the priority for an MSTI, only the four most significant bits are used.
- To configure the port priority with this command, specify the instance (**cist**, **msti**, or **vlan**), a port number or link aggregate ID that is associated with that instance, and the priority value.
- The port priority value configured with this command is only applied to the specified instance. As a result, a single port can have different priority values for each instance. For example, in flat mode, port 1/24 can have a priority value of 7 for MSTI 2 and a priority value of 5 for MSTI 3.
- The port priority specifies the value of the priority field contained in the first byte of the port ID. The second byte contains the physical switch port number.

Examples

The following command examples set the bridge priority for the specified instance:

```
-> spantree priority 8192
-> spantree cist priority 8192
-> spantree vlan 2 priority 32679
-> spantree msti 1 priority 2500
ERROR: Valid bridge priority values are multiples of 4096: 0, 4096,
         8192, 12288, 16384 ... 61440
-> spantree msti 1 priority 8192
```

The following command examples set the port priority for the specified instance:

```
-> spantree port 1/10 priority 10
-> spantree cist port 1/10 priority 10
-> spantree cist linkagg 10 priority 1
-> spantree vlan 200 port 2/1 priority 15
-> spantree vlan 2 linkagg 5 priority 2
-> spantree msti 2 port 1/24 priority 5
-> spantree msti 3 linkagg 6-8 priority 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.
show spantree ports	Displays the Spanning Tree port configuration.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsPriority
   vStpInsBridgeAddress
```

spantree hello-time

Configures the Spanning Tree hello time value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN mode VLAN instance. This value specifies the amount of time, in seconds, between each transmission of a BPDU on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root.

spantree [cist | vlan *vlan_id***] hello-time** *seconds*

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
vlan_id	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
seconds	Specifies the Hello time value in seconds. The valid range is 1–10.

Defaults

By default, the bridge hello time value is set to 2 seconds.

parameter	default
cist | vlan *vlan_id*	**cist**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Lowering the Hello Time interval improves the robustness of the Spanning Tree Algorithm. Increasing the Hello Time interval lowers the overhead of the Spanning Tree Algorithm.
- If the optional **cist** or **vlan** parameter is not specified with this command, the hello time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the **cist** and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified hello time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.
- Note that for Multiple Spanning Tree Instances (MSTI), the hello time value is inherited from the CIST instance and is not a configurable parameter.

Examples

```
-> spantree hello-time 5
-> spantree cist hello-time 5
-> spantree vlan 10 hello-time 3
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsBridgeHelloTime
```

spantree max-age

Configures the bridge maximum age time value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN mode VLAN instance. This value is the amount of time, in seconds, that the Spanning Tree Protocol information learned from the network on any port is retained. This information is discarded when it ages beyond the maximum age value.

spantree [cist | vlan *vlan_id***] max-age** *seconds*

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
vlan_id	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
seconds	Max-age time in seconds. The valid range is 6–40.

Defaults

By default, the bridge maximum age time value is set to 20 seconds.

parameter	default
cist | vlan *vlan_id*	**cist**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- A low maximum age time causes the Spanning Tree Algorithm to reconfigure more often.
- If the optional **cist** or **vlan** parameter is not specified with this command, the maximum age time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the **cist** and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified maximum age time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.
- Note that for Multiple Spanning Tree Instances (MSTI), the maximum age time value is inherited from the CIST instance and is not a configurable parameter.

Examples

```
-> spantree max-age 10
-> spantree cist max-age 10
-> spantree vlan 10 max-age 30
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsBridgeMaxAge
```

spantree forward-delay

Configures the bridge forward delay time for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN mode VLAN instance. This value is the amount of time, in seconds, that determines how fast a port changes its Spanning Tree state until it reaches a forwarding state. The forward delay time specifies how long a port stays in the listening and learning states, which precede the forwarding state.

spantree [cist | vlan *vlan_id***] forward-delay** *seconds*

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
vlan_id	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
seconds	Forward delay time, in seconds.The valid range is 4–30.

Defaults

By default, the bridge forward delay time value is set to 15 seconds.

parameter	default
cist | vlan *vlan_id*	**cist**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- A low forward delay time can cause temporary loops in the network, because data may get forwarded before the reconfiguration message has reached all nodes on the network.
- The forward delay time is also used to age out all dynamic MAC address entries in the forwarding table (MAC address table) when a topology change occurs.
- If the optional **cist** or **vlan** parameter is not specified with this command, the forward delay time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the **cist** and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified forward delay time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.
- Note that for Multiple Spanning Tree Instances (MSTI), the forward delay time is inherited from the CIST instance and is not a configurable parameter.

Examples

```
-> spantree forward-delay 30
-> spantree cist forward-delay 30
-> spantree vlan 5 forward-delay 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsBridgeForwardDelay
```

spantree bpdu-switching

Enables or disables the switching of Spanning Tree BPDU for VLAN and CIST instances if the switch is running in the per-VLAN mode.

spantree {vlan *vlan_id* **| cist} bpdu-switching {enable | disable}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
enable	Enables BPDU switching for the specified instance.
disable	Disables BPDU switching for the specified instance.

Defaults

By default, BPDU switching is disabled for VLAN or CIST instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specifying the BPDU switching status for a VLAN does not depend on the current VLAN Spanning Tree status. For example, setting the BPDU switching status to enabled is allowed on a VLAN that also has Spanning Tree enabled.
- Use the **vlan** parameter along with the *vlan_id* to enable or disable BPDU switching for a particular VLAN.
- Use the **cist** parameter to enable or disable BPDU switching for the CIST instance.

Examples

```
-> spantree mode flat
-> spantree bpdu-switching enable
-> spantree bpdu-switching disable
-> spantree cist bpdu-switching enable
-> spantree cist bpdu-switching disable

-> spantree mode per-vlan
-> spantree vlan 10 bpdu-switching enable
-> spantree vlan 10 bpdu-switching disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan members untagged	Enables or disables Spanning Tree instance for the specified VLAN.
show spantree	Displays VLAN Spanning Tree parameter values.

MIB Objects

```
vStpInsTable
   vStpInsBpduSwitching
```

spantree path-cost-mode

Configures the automatic selection of a 16-bit path cost for STP/RSTP ports and a 32-bit path cost for MSTP ports or sets all path costs to use a 32-bit value.

spantree path-cost-mode {auto | 32bit}

Syntax Definitions

auto	The port path cost value is automatically set depending on which protocol is active on the switch (32-bit for MSTP, 16-bit for STP/RSTP).
32bit	Specifies that a 32-bit value is used for the port path cost value regardless of which protocol is active on the switch.

Defaults

By default, the path cost mode is set to **auto**.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- All path cost values, except those for MSTIs, are reset to the default path cost value when this mode is changed.
- When connecting a switch running in the 32-bit path cost mode to a switch running in the 16-bit mode, the 32-bit switch has a higher path cost value and thus an inferior path cost to the 16-bit switch. To avoid this, use the **spantree path-cost-mode** command to change the 32-bit switch to a 16-bit switch.
- Note that when the protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values. The exception to this is if the path cost mode is set to 32-bit prior to the protocol change, the path cost is not reset to its default value

Examples

```
-> spantree path-cost-mode 32bit
-> spantree path-cost-mode auto
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree protocol	Configures the protocol for the flat mode CIST instance or a per-VLAN mode VLAN instance.

MIB Objects

```
vStpBridge
   vStpPathCostMode
```

spantree pvst+compatibility

Enables or disables PVST+ mode on the switch, port or link aggregate enabling them to operate with Cisco switches.

spantree pvst+compatibility {port *chassis/slot/port***] | linkagg** *agg_id***} {enable | disable | auto}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot number and port number of the physical port.
*agg_id***[-***agg_id2***]**	The link aggregate ID number.
enable	Enables the PVST+ mode.
disable	Disables the PVST+ mode.
auto	IEEE BPDUs are used until a PVST+ BPDU is detected.

Defaults

PVST+ is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- In order to handle PVST+ mode, the ports must be configured in per-VLAN mode.
- Specify **pvst+compatibility enable** to enable all the ports on the switch to handle PVST+ BPDUs.
- Initially, a port sends or receive IEEE BPDUs. Once a PVST+ BPDU is received, the port sends and receives only PVST+ BPDUs for tagged VLANs and IEEE BPDUs for default VLANs.

Examples

```
-> spantree pvst+compatibility enable
-> spantree pvst+compatibility disable
-> spantree port 1/3 pvst+compatibility enable
-> spantree port 2/2 pvst+compatibility auto
-> spantree linkagg 2 pvst+compatibility enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree	Displays Spanning Tree bridge information for all flat mode Common and Internal Spanning Tree (CIST) instance and per-VLAN mode VLAN instance.
show spantree ports	Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance or a per-VLAN mode VLAN instance.
show spantree cist ports	Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance.
show spantree msti ports	Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).

MIB Objects

```
vStpPortConfigPVST
vStpPortConfigStatePVST
vStpBridgeModePVST
```

spantree auto-vlan-containment

Enables or disables Auto VLAN Containment (AVC). When enabled, AVC prevents a port that has no VLANs mapped to an Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Such ports are automatically assigned an infinite path cost value to make them an inferior choice for root port.

spantree [msti *msti_id***] auto-vlan-containment {enable | disable}**

Syntax Definitions

msti_id	An existing MSTI ID number. A range of VLANs are associated to an MSTI ID number.
enable	Enables automatic VLAN containment.
disable	Disables automatic VLAN containment.

Defaults

By default, automatic VLAN containment is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The AVC feature is not active for any MSTI until it is globally enabled. To globally enable this feature, use the **spantree auto-vlan-containment** command but do not specify an *msti_ id*.
- When AVC is globally enabled, it is active for all MSTIs. To disable AVC for a single instance, specify the *msti_id* for the instance and use the **disable** form of this command.
- Use the **enable** form of this command and specify an *msti_id* to enable AVC for an instance that was previously disabled.
- An administratively set port path cost takes precedence and prevents AVC configuration of the path cost. However, if the port path cost is administratively set to zero, then the path cost is reset to the default value.
- Note that when AVC is disabled, a port assigned to a VLAN that is not mapped to a specific instance, can become the root port for that instance and cause a loss of connectivity between other VLANs.
- AVC does not have any effect on root bridges.

Examples

```
-> spantree auto-vlan-containment enable
-> spantree auto-vlan-containment disable
-> spantree msti 1 auto-vlan-containment disable
-> spantree msti 1 auto-vlan-containment enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree msti ports	Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).

MIB Objects

```
vStpInsTable
   vStpInsAutoVlanContainment
vStpBridge
   vStpBridgeAutoVlanContainment
```

spantree cist

Enables or disables the Spanning Tree status on a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance.

spantree cist {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables Spanning Tree on the specified port for the CIST instance.
disable	Disables Spanning Tree on the specified port for the CIST instance.

Defaults

By default, the Spanning Tree status is enabled on eligible ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the CIST instance regardless of which Spanning Tree operating mode (flat or per-VLAN) or protocol is active for the switch.
- If the switch is running in per-VLAN mode when this command is used, the Spanning Tree status configured for the port is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- When the Spanning Tree status is disabled on a port, the port is set to a forwarding state for the specified instance.
- Physical ports that are reserved for link aggregation do not participate in the Spanning Tree Algorithm. Instead, the algorithm is applied to the aggregate logical link (virtual port) that represents a collection of physical ports.

Examples

```
-> spantree cist port 4/1 enable
-> spantree cist port 4/2-5 disable
-> spantree cist linkagg 16 disable
-> spantree cist linkagg 22-26 enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree vlan	Configures the Spanning Tree status on a port or a link aggregate of ports for a VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortEnable
```

spantree vlan

Enables or disables the Spanning Tree status on a port or a link aggregate of ports for the specified VLAN instance.

spantree vlan *vlan_id* **[**-*vlan2***] {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} {enable | disable}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables Spanning Tree on the specified port for the specified instance.
disable	Disables Spanning Tree on the specified port for the specified instance.

Defaults

By default, the Spanning Tree status is enabled on eligible ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which Spanning Tree operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the Spanning Tree status configured for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the per-VLAN mode.
- When the Spanning Tree status is disabled on a port, the port is set to a forwarding state for the specified instance.
- If STP is disabled on a VLAN in the per-VLAN mode, the port Spanning Tree status is ignored and all active ports associated with the VLAN are put in a forwarding state and not included in the Spanning Tree Algorithm. Note that when this occurs, ports will *not* bridge BPDU unless the BPDU switching status for the VLAN is enabled.
- Physical ports that are reserved for link aggregation do not participate in the Spanning Tree Algorithm. Instead, the algorithm is applied to the aggregate logical link (virtual port) that represents a collection of physical ports.

Examples

```
-> spantree vlan 2 port 4/1 enable
-> spantree vlan 2 port 4/2-5 disable
```

```
-> spantree vlan 3 linkagg 16 disable
-> spantree vlan 3 linkagg 22-25 disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist	Configures the Spanning Tree status on a port or an aggregate of ports for the CIST instance when the switch is operating in either the per-VLAN or flat mode.
spantree vlan admin-state	Enables or disables Spanning Tree instance for the specified VLAN.
spantree bpdu-switching	Enables or disables the switching of Spanning Tree BPDU for all VLAN instances if the switch is running in the per-VLAN mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortEnable
```

spantree cist path-cost

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

spantree cist {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} path-cost** *path_cost*

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
path_cost	Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the port path cost value for the CIST instance regardless of which operating mode (flat or per-VLAN) or protocol is active for the switch.
- If the switch is running in per-VLAN mode when this command is used, the specified path cost value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when the Spanning Tree protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.
- Use the **spantree path-cost-mode** command to automatically select the path cost value based on the active Spanning Tree protocol (16-bit for STP and RSTP, 32-bit for MSTP) or to use a 32-bit path cost value regardless of which protocol is active.
- If the *path_cost* is set to zero, there are recommended 16-bit and 32-bit values which are used by default depending on the link speed. Refer to the “Configuring Spanning Tree Parameters” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for a list of values.

Examples

```
-> spantree cist port 4/1 path-cost 19
-> spantree cist port 4/2-5 path-cost 19
-> spantree cist linkagg 16 path-cost 12000
-> spantree cist linkagg 17-20 path-cost 12000
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree path-cost-mode	Selects a 32-bit or automatic path cost mode for the switch.
spantree msti path-cost	Configures the Spanning Tree path cost value for a port or a link aggregate of ports for an MSTI.
spantree vlan path-cost	Configures the Spanning Tree path cost value for a port or a link aggregate of ports for a VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

spantree msti path-cost

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the specified flat mode Multiple Spanning Tree Instance (MSTI). This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

spantree msti *msti_id* **{port** *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} path-cost** *path_cost*

Syntax Definitions

msti_id	An existing MSTI ID number. If MSTI 0 is specified, the priority applies to the CIST instance.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
path_cost	Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the specified MSTI regardless of which operating mode (flat or per-VLAN) is active for the switch. However, if MSTP is not the selected flat mode protocol, the path cost value for any MSTI is not configurable.
- Note that if zero is entered for the *msti_id* value, the specified path cost value is applied to the CIST instance.
- Note that when the Spanning Tree protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.
- The path cost value configured with this command is only applied to the specified instance. As a result, a single port can have a different path cost for each instance. For example, in flat mode, port 1/24 can have a path cost of 20000 for MSTI 2 and a path cost of 35000 for MSTI 3.
- If the switch is running in per-VLAN mode when this command is used, the specified path cost value is not active for the specified MSTI until the operating mode for the switch is changed to the flat mode.
- When MSTP is the active protocol on the switch, only a 32-bit path cost value is used. Using a 16-bit path cost value is not an option.

- If the *path_cost* is set to zero, there are recommended 16-bit and 32-bit values which are used by default depending on the link speed. Refer to the "**Configuring Spanning Tree Parameters**" chapter for a list of values.

Examples

```
-> spantree msti 0 port 4/1 path-cost 35000
-> spantree msti 0 port 1/20-24 path-cost 12000
-> spantree msti 2 linkagg 10 path-cost 20000
-> spantree msti 2 linkagg 10-12 path-cost 65000
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist path-cost	Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the CIST instance.
spantree vlan path-cost	Configures the Spanning Tree path cost value for a port or a link aggregate of ports for a VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

spantree vlan path-cost

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the specified VLAN instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

spantree vlan *vlan_id* **{port** *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id* **[**-*agg_id2***]} path-cost** *path_cost*

Syntax Definitions

vlan_id	An existing VLAN ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
path_cost	Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified path cost for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the per-VLAN mode.
- Note that when the Spanning Tree protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.
- Use the **spantree path-cost-mode** command to automatically select the path cost value based on the active Spanning Tree protocol (16-bit for STP and RSTP, 32-bit for MSTP) or to use a 32-bit path cost value regardless of which protocol is active.
- If the *path_cost* is set to zero, there are recommended 16-bit and 32-bit values which are used by default depending on the link speed. Refer to the "**Configuring Spanning Tree Parameters**" chapter for a list of values.

Examples

```
-> spantree vlan 200 port 4/1 path-cost 4
-> spantree vlan 200 port 4/2-5 path-cost 4
```

```
-> spantree vlan 300 linkagg 16 path-cost 200000
-> spantree vlan 500 linkagg 24-28 path-cost 20000
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist path-cost	Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the CIST instance.
spantree msti path-cost	Configures the Spanning Tree path cost value for a port or a link aggregate of ports for an MSTI.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

spantree cist mode

Configures manual mode (forwarding or blocking) or dynamic mode to manage the state of a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

spantree cist {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} mode {forwarding | dynamic | blocking}**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
forwarding	Sets the port state to forwarding.
dynamic	Port state is determined by the Spanning Tree algorithm.
blocking	Sets the port state to blocking.

Defaults

By default, the port Spanning Tree mode is set to dynamic.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the port Spanning Tree mode for the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in per-VLAN mode when this command is used, the specified port mode is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Ports manually configured to operate in a forwarding or blocking state do not participate in the Spanning Tree algorithm.
- When port state is manually set to forwarding or blocking, the port remains in that state until it is changed using this command.

Examples

```
-> spantree cist port 4/1 mode forwarding
-> spantree cist port 4/2-5 mode forwarding
-> spantree cist linkagg 10 mode blocking
-> spantree cist linkagg 15-20 mode forwarding
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree loop-guard	Configures the Spanning Tree mode for a port or a link aggregate of ports for the specified VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortManualMode
```

spantree loop-guard

Enables or disables the STP loop-guard on a port or link aggregate.

spantree {port *chassis/slot/port***[-***port2***]** | **linkagg** *linkagg_id* **[-***linkagg_id2***]} loop-guard {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports.
*linkagg_id***[-***linkagg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (example 10-20).
enable	Enables STP loop-guard.
disable	Disables STP loop-guard.

Defaults

STP loop-guard is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When you enable loop-guard on a port, it is automatically applied to all the active instances or VLANs associated to the port.
- Loop-guard cannot be enabled on a port if root-guard is already enabled on the port or link aggregate related to the port. Root-guard must be disabled before configuring loop-guard. Similarly, when loop-guard configuration is enabled on a port or chassis, root-guard cannot be configured on the port/s.
- Loop-guard can be enabled on all types of ports including designated (forwarding), non-designated (alternate, secondary, or root) ports. However, STP loop-guard configuration does not affect designated ports. Hence, loop-guard is not effective when applied on designated ports.
- When loop-guard is enabled on root ports, they change to blocking mode when a loop-guard error occurs. In such an instance, the alternate or secondary ports takeover until the root port recovers from the error state.
- If a set of ports that are already blocked by loop-guard are grouped together to form a link aggregate, the new link aggregate gets a new designated role. The link aggregate can also obtain a forwarding state depending on the STP state.
- If a spanning tree channel is blocked by loop-guard and the channel breaks, spanning tree loses all the state information. The individual physical ports obtain the designated role, even if one or more of the links that formed the channel are unidirectional. New link aggregate might obtain a forwarding state but new port state is defined.

- The ports that are configured as fast-forwarding or edge-ports do not receive BPDUs. Loop-guard is not effective on such ports.
- Loop-guard error state is recovered when the administrative state of the port is enabled or disabled.
- When a VLAN is disabled, all the VLAN port associations recover from the error state.
- The loop-guard feature can be enabled on the ports that have STP (RSTP, MRSTP or MSTP) enabled.
- STP loop-guard on link aggregate protects all ports that are members of the link aggregation group.

Examples

```
-> spantree port 1/1/2 loop-guard enable
-> spantree linkagg 1 loop-guard enable
-> spantree port 1/1/2 loop-guard disable
-> spantree linkagg 1 loop-guard disable
```

Release History

Release 8.2.1; command introduced.

Related Commands

show spantree ports	Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance.

MIB Objects

```
vStpPortConfigTable
   vStpPortConfigIfIndex
   vStpPortConfigLoopGuard
```

spantree vlan mode

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or a link aggregate of ports for the specified VLAN instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

spantree vlan *vlan_id* **{port** *chassis/slot/port***[-***port2***]** | **linkagg** *agg_id* **[-***agg_id2***]} mode {dynamic | blocking | forwarding}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
chassis	The chassis identifier when running in virtual chassis mode.
*slot/port***[-***port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
dynamic	Port state is determined by the Spanning Tree algorithm.
blocking	Sets the port state to blocking.
forwarding	Sets the port state to forwarding.

Defaults

By default, the port Spanning Tree mode is set to dynamic.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified mode for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the per-VLAN mode.
- Ports manually configured to operate in a forwarding or blocking state do not participate in the Spanning Tree algorithm.
- When port state is manually set to forwarding or blocking, the port remains in that state until it is changed using this command.

Examples

```
-> spantree vlan 255 port 4/1-4 mode forwarding
-> spantree vlan 355 port 1/24 mode dynamic
-> spantree vlan 450 linkagg 1 mode dynamic
-> spantree vlan 450 linkagg 1-5 mode dynamic
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist mode	Configures the Spanning Tree mode for a port or a link aggregate of ports for the CIST instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortManualMode
```

spantree cist connection

Configures the connection type for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

spantree cist {port *chassis/slot/port* **[**-*port2***] | linkagg** *agg_id* **[**-*agg_id2***]} connection {noptp | ptp | autoptp}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software automatically defines connection type as point-to-point or no point-to-point.

Defaults

By default, the link connection type is set to auto point-to-point.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the port connection type for the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in per-VLAN mode when this command is used, the specified port connection type is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- A port is considered connected to a point-to-point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines the port must run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point-to-point LAN segment.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point-to-point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

Examples

```
-> spantree cist port 7/24 connection noptp
-> spantree cist port 7/25-28 connection ptp
```

```
-> spantree cist linkagg 5-10 connection autoptp
-> spantree cist linkagg 5-10 connection autoptp
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the flat mode CIST instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

spantree vlan connection

Configures the connection type for a port or a link aggregate of ports for a VLAN instance.

spantree vlan *vlan_id* **{port** *chassis/slot/port* **[**-*port2***]** | **linkagg** *agg_id* **[**-*agg_id2***]} connection {noptp | ptp | autoptp}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software automatically defines connection type as point-to-point or no point-to-point.

Defaults

By default, the link connection type is set to auto point-to-point.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified connection type for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the per-VLAN mode.
- A port is considered connected to a point-to-point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines the port must run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point-to-point LAN segment.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

Examples

```
-> spantree vlan 255 port 7/24 connection noptp
-> spantree vlan 255 port 7/25-27 connection ptp
-> spantree vlan 255 linkagg 3 connection autoptp
-> spantree vlan 255 linkagg 3-7 connection autoptp
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the flat mode CIST instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

spantree cist admin-edge

Configures the administrative edge port status for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

spantree cist {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} admin-edge {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables the administrative edge port status for the specified port-CIST instance.
disable	Disables the administrative edge port status for the specified port-CIST instance.

Defaults

By default, the administrative edge port status is disabled (off).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the port connection type for the CIST instance regardless of which operating mode (flat or per-VLAN) is active on the switch.
- If the switch is running in the per-VLAN mode when this command is used, the specified edge port status is not active for the CIST instance until the switch is configured to run in the flat Spanning Tree mode.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that connect to a host (PC, workstation, server, and so on) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point-to-point connection type.

Examples

```
-> spantree cist linkagg 15 admin-edge enable
-> spantree cist linkagg 4-10 admin-edge enable
-> spantree cist port 8/25 admin-edge disable
-> spantree cist port 2/2-5 admin-edge enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch
spantree vlan admin-edge	Configures the administrative edge port status for a port or a link aggregate of ports for a specific VLAN instance.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or a link aggregate of ports for the flat mode CIST instance.
spantree vlan auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or a link aggregate of ports for the specified per-VLAN mode VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminEdge
```

spantree vlan admin-edge

Configures the administrative edge port status for a port or a link aggregate of ports for a VLAN instance.

spantree vlan *vlan_id* **{port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} admin-edge {enable | disable}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables the administrative edge port status for the specified port-VLAN instance.
disable	Disables the administrative edge port status for the specified port-VLAN instance.

Defaults

By default, the administrative edge port status is disabled (off).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified edge port status for the port is not active for the VLAN instance until the switch is configured to run in the per-VLAN Spanning Tree mode.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point to point connection type.

Examples

```
-> spantree vlan 4 linkagg 15 admin-edge enable
-> spantree vlan 5 linkagg 12-14 admin-edge enable
-> spantree vlan 255 port 8/23 admin-edge disable
-> spantree vlan 3 port 2/2-5 admin-edge enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or aggregate of ports for the flat mode CIST instance.
spantree vlan auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminEdge
```

spantree cist auto-edge

Configures whether or not Spanning Tree automatically determines the operational edge port status of a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

spantree cist {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id* **[**-*agg_id2***]} auto-edge {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Spanning Tree automatically determines edge port status.
disable	Spanning Tree does not automatically determine edge port status.

Defaults

By default, automatic edge port status configuration is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the per-VLAN mode when this command is used, the specified edge port status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree mode.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the connection type of the port is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point to point connection type.

Examples

```
-> spantree cist linkagg 15 auto-edge enable
-> spantree cist linkagg 10-12 auto-edge disable
-> spantree cist port 8/23 auto-edge disable
-> spantree cist port 2/2-5 auto-edge enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch
spantree vlan auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree vlan admin-edge	Configures the administrative edge port status for a port or aggregate of ports for a specific VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAutoEdge
```

spantree vlan auto-edge

Configures whether or not Spanning Tree determines the operational edge port status for a port or a link aggregate of ports for the specified per-VLAN mode VLAN instance.

spantree vlan *vlan_id* **{port** *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id* **[**-*agg_id2***]} auto-edge {enable | disable}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
chassis	The chassis identifier when running in virtual chassis mode.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Spanning Tree automatically determines edge port status.
disable	Spanning Tree does not automatically determine edge port status.

Defaults

By default, automatic edge port status configuration is enabled (on).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified edge port status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the connection type of the port is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point to point connection type.

Examples

```
-> spantree vlan 255 port 8/23 auto-edge disable
-> spantree vlan 4 port 2/2-10 auto-edge enable
-> spantree vlan 100 linkagg 10 auto-edge disable
-> spantree vlan 200 linkagg 1-5 auto-edge enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or aggregate of ports for the flat mode CIST instance.
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree vlan admin-edge	Configures the administrative edge port status for a port or aggregate of ports for a specific VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAutoEdge
```

spantree cist restricted-role

Configures the restricted role status for a port or a link aggregate of ports. Enabling this parameter blocks the port from becoming the Root Port, even if it is the most likely candidate for root. Once a root port is selected, the restricted port is selected as an Alternate Port.

spantree cist {port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} restricted-role {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables the restricted role status for the specified port.
disable	Disables the restricted role status for the specified port.

Defaults

By default, the restricted role status for the port is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When running in flat mode, this is a per-port setting and is applicable to any CIST or MSTI instances configured on that port.
- Enabling the restricted role status is used by network administrators to prevent bridges external to the core region of the network from influencing the Spanning Tree topology.
- Note that enabling the restricted role status for a port may impact connectivity within the network.

Examples

```
-> spantree cist linkagg 15-20 restricted-role enable
-> spantree cist port 8/23 restricted-role disable
-> spantree cist port 8/24-27 restricted-role disable
-> spantree cist linkagg 10 restricted-role disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree vlan restricted-role	Configures the restricted role status for a port or aggregate of ports for the per-VLAN mode VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortRestrictedRole
```

spantree vlan restricted-role

Configures the restricted role status for a port or a link aggregate of ports for the specified VLAN instance. Enabling this parameter blocks the port from becoming the Root Port, even if it is the most likely candidate for root. Once a Root Port is selected, the restricted port is selected as an Alternate Port.

spantree vlan *vlan_id* **{port** *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} restricted-role {enable | disable}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables the restricted role status for the specified port-VLAN instance.
disable	Disables the restricted role status for the specified port-VLAN instance.

Defaults

By default, the restricted role status for the port is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enabling the restricted role status is used by network administrators to prevent bridges external to the core region of the network from influencing the Spanning Tree topology.
- Note that enabling the restricted role status for a port may impact connectivity within the network.
- This command only applies to the VLAN instance specified by the VLAN ID regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified restricted role status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.

Examples

```
-> spantree vlan 3 linkagg 15 restricted-role enable
-> spantree vlan 255 port 8/23 restricted-role enable
-> spantree vlan 255 port 8/24-27 restricted-role enable
-> spantree vlan 255 linkagg 11-15 restricted-role enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist restricted-role	Configures the restricted role status for a port or aggregate of ports for the flat mode CIST instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortRestrictedRole
```

spantree cist restricted-tcn

Configures the restricted TCN status for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST). When this parameter is enabled, the port does not propagate topology changes and notifications to/from other ports.

spantree cist {port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} restricted-tcn {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables the restricted TCN status for the specified port-CIST instance.
disable	Disables the restricted TCN status for the specified port-CIST instance.

Defaults

By default, the restricted TCN status for the port is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enabling the restricted TCN status is used by network administrators to prevent bridges external to the core region of the network from causing unnecessary MAC address flushing in that region.
- Note that enabling the restricted TCN status for a port may impact Spanning Tree connectivity.
- This command only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the per-VLAN mode when this command is used, the specified restricted TCN status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree mode.

Examples

```
-> spantree cist linkagg 15 restricted-tcn enable
-> spantree cist port 8/23 restricted-tcn disable
-> spantree cist port 2/2-4 restricted-tcn enable
-> spantree cist linkagg 10-14 restricted-tcn disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree vlan restricted-tcn	Configures the restricted TCN status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortRestrictedTcn
```

spantree vlan restricted-tcn

Configures the restricted TCN status for a port or a link aggregate of ports for the specified VLAN instance. When this parameter is enabled, the port does not propagate topology changes and notifications to/from other ports.

spantree vlan *vlan_id* **{port** *chassis/slot/port* **[**-*port2***]** | **linkagg** *agg_id* **[**-*agg_id2***]} restricted-tcn {enable | disable}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8)**.**
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables the restricted TCN status for the specified port-VLAN instance.
disable	Disables the restricted TCN status for the specified port-VLAN instance.

Defaults

By default, the restricted TCN is set to disable.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enabling the restricted TCN status is used by network administrators to prevent bridges external to the core region of the network from causing unnecessary MAC address flushing in that region.
- Note that enabling the restricted TCN status for a port may impact Spanning Tree connectivity.
- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified restricted TCN status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.

Examples

```
-> spantree vlan 2 linkagg 15 restricted-tcn enable
-> spantree vlan 2 linkagg 16-20 restricted-tcn enable
-> spantree vlan 255 port 8/23 restricted-tcn disable
-> spantree vlan 255 port 8/24-27 restricted-tcn disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist restricted-tcn	Configures the restricted TCN status for a port or aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortRestrictedTcn
```

spantree cist txholdcount

This command is used to rate limit the transmission of BPDU through a given port for the flat mode Common and Internal Spanning Tree (CIST) instance.

spantree cist txholdcount *value*

Syntax Definitions

value	A numeric value that controls the transmission of BPDU through the port. The valid range is 1–10.

Defaults

By default, the **txholdcount** value is set to 3.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the per-VLAN mode when this command is used, the specified **txholdcount** status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree mode.

Examples

```
-> spantree cist txholdcount 5
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree vlan txholdcount	Configures the BPDU transmission rate limit for the specified VLAN instance.

MIB Objects

```
vStpInsTable
   vStpInsBridgeTxHoldCount
```

spantree vlan txholdcount

This command is used to rate limit the transmission of BPDU through a given port for the VLAN instance.

spantree vlan *vlan_id* **txholdcount {***value***}**

Syntax Definitions

vlan_id	An existing VLAN ID number.
value	A numeric value that controls the transmission of BPDU through the port. The valid range is 1–10.

Defaults

By default, the **txholdcount** value is set to 3.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified **txholdcount** status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.

Examples

```
-> spantree vlan 3 txholdcount 6
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist txholdcount	Configures the BPDU transmission rate limit for the CIST instance.

MIB Objects

```
vStpInsTable
   vStpInsBridgeTxHoldCount
```

show spantree

Displays Spanning Tree bridge information for the flat mode Common and Internal Spanning Tree (CIST) instance or the per-VLAN mode VLAN instances.

show spantree

Syntax Definitions

N/A

Defaults

NA

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the switch is operating in the per-VLAN mode, this command displays a list of VLAN instances.
- If the switch is operating in the flat mode and the protocol is STP or RSTP, this command displays the single flat mode instance.
- If the switch is operating in the flat mode and the protocol is set to MSTP, this command displays a list of MSTIs, including MSTI 0 (also known as the CIST).

Examples

```
-> spantree mode flat
-> spantree protocol rstp
-> show spantree

Spanning Tree Path Cost Mode :  32 BIT
Bridge STP Status Protocol Priority(Prio:SysID)
------+----------+--------+--------------------
     1      ON      RSTP   32768 (0x8000:0x0000)
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **spantree path-cost-mode** command.
Bridge	The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol.
STP Status	The Spanning Tree state for the CIST instance (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to the instance (**STP** or **RSTP**). Configured through the **spantree protocol** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **spantree priority** command.

```
-> spantree mode flat
-> spantree protocol mstp

-> show spantree
  Spanning Tree Path Cost Mode : AUTO
 Msti STP Status Protocol Priority (Prio:SysID)
-----+----------+--------+--------------------
    0      ON      MSTP   32768 (0x8000:0x0000)
    2      ON      MSTP   32770 (0x8000:0x0002)
    3      ON      MSTP   32771 (0x8000:0x0003)
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**). Configured through the **spantree path-cost-mode** command.
Msti	The Multiple Spanning Tree Instance (MSTI) instance number. Configured through the **spantree msti** command. Note that MSTI 0 also represents the CIST instance that is always present on the switch.
STP Status	The Spanning Tree state for the MSTI (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to this instance. Configured through the **spantree protocol** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **spantree priority** command.

```
-> spantree mode per-vlan
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+-------------
    1      ON       RSTP   32768 (0x8000)
  200      ON       RSTP   32768 (0x8000)
  500     OFF       RSTP   32768 (0x8000)
 4094     OFF       RSTP   32768 (0x8000)
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**). Configured through the **spantree path-cost-mode** command.
Vlan	The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the **vlan** commands
STP Status	The Spanning Tree state for the instance (**ON** or **OFF**). Configured through the **spantree vlan admin-state** command.
Protocol	The Spanning Tree protocol applied to this instance (**STP** or **RSTP**). Configured through the **spantree protocol** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **spantree priority** command.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree cist	Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree msti	Displays the Spanning Tree bridge configuration for an MSTI regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree vlan	Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsProtocolSpecification
   vStpInsMode
   vStpInsPriority
   vStpInsBridgeAddress
   vStpInsDesignatedRoot
   vStpInsRootCost
   vStpInsRootPortNumber
   vStpInsNextBestRootCost
   vStpInsNextBestRootPortNumber
   vStpInsBridgeTxHoldCount
   vStpInsTopChanges
   vStpInsTimeSinceTopologyChange
   vStpInsMaxAge
   vStpInsForwardDelay
   vStpInsHelloTime
```

show spantree cist

Displays the Spanning Tree bridge configuration for the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guideline

This command displays Spanning Tree bridge information for the flat mode CIST instance regardless of which mode (per-VLAN or flat) is active on the switch. Note that minimal information is displayed when this command is used in the per-VLAN mode, as the CIST is not active in this mode. See the second example below.

Examples

```
-> spantree mode flat
-> show spantree cist
Spanning Tree Parameters for Cist
  Spanning Tree Status :                   ON,
  Protocol             :       IEEE Multiple STP,
  mode                 :    FLAT (Single STP),
  Auto-Vlan-Containment:           Enabled   ,
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-2c:fa:a2:24:87:51,
  CST Designated Root  :   8000-00:e0:b1:cf:26:3d,
  Cost to CST Root     :                 2000,
  Designated Root      :   8000-2c:fa:a2:24:87:51,
  Cost to Root Bridge  :                    0,
  Root Port            :               1/1/46,
  TxHoldCount          :                    3,
  Topology Changes     :                   10,
  Topology age         :            00:01:10,
  Last TC Rcvd Port    :               1/1/46,
  Last TC Rcvd Bridge  :   8000-00:e0:b1:cf:26:3d,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
```

```
      System Hello Time    =     2

-> spantree mode per-vlan
-> show spantree cist
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters for Cist
  Spanning Tree Status :                ON,
  Protocol             :       IEEE Multiple STP,
  Priority             :    32768 (0x8000),
  TxHoldCount          :                 5,
  System Max Age (seconds)       =      10,
  System Forward Delay (seconds) =      10,
  System Hello Time (seconds)    =       5
```

output definitions

Spanning Tree Status	The Spanning Tree state for the instance (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to the CIST (**STP, RSTP,** or **MSTP**). Configured through the **spantree protocol** command.
Mode	The Spanning Tree operating mode for the switch (**per-vlan** or **flat**). Configured through the **spantree mode** command.
Auto-Vlan-Containment	The auto VLAN containment status for the instance (**Enabled** or **Disabled**). AVC prevents a port that has no VLANs mapped to a Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Configured through the **spantree auto-vlan-containment** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **spantree priority** command.
Bridge ID	The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.
CST Designated Root	The bridge identifier for the root of the flat mode CIST instance. This field only appears when MSTP is active on the switch.
Cost to CST Root	The cost of the path to the root of the flat mode CIST instance. This field only appears when MSTP is active on the switch.
Designated Root	The bridge identifier for the root of the Spanning Tree for this instance.
Cost to Root Bridge	The cost of the path to the root for this Spanning Tree instance.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
Tx Hold Count	The count to limit the transmission of BPDU through the port.
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.
Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (**hh:mm:ss** or **dd days and hh:mm:ss**).
Last TC Rcvd Port	The port that received the TC Flag Set in RSTP or MSTP protocol BPDU. Default value is None.

output definitions (continued)

Last TC Rcvd Bridge	The adjacent designated bridge ID received from TC Flag Set in RSTP or MSTP BPDU along with Last TC Rcvd Port. This information is provided only for active RSTP and MSTP topologies. Default value is None.
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the **spantree max-age** command.
Forward Delay	The amount of time (in seconds) that a port remains in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **spantree forward-delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **spantree hello-time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Hello Time	The Hello Time value for the root bridge.
BPDU Switching Enabled	The status of BPDU switching for the instance. This field only appears when BPDU switching is enabled. Configured through the **spantree bpdu-switching** command.

Release History

Release 7.1.1; command introduced.
Release 8.4.1; **Topology Change Port** field added.
Release 8.5R4; **Last TC Rcvd Bridge** field added.

Related Commands

show spantree	Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.
show spantree msti	Displays the Spanning Tree bridge configuration for an MSTI regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree vlan	Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsProtocolSpecification
   vStpInsPriority
   vStpInsBridgeAddress
   vStpInsTimeSinceTopologyChange
   vStpInsTopChanges
   vStpInsDesignatedRoot
   vStpInsRootCost
   vStpInsRootPortNumber
   vStpInsNextBestRootCost
   vStpInsNextBestRootPortNumber
   vStpInsMaxAge
   vStpInsHelloTime
   vStpInsBridgeTxHoldCount
   vStpInsForwardDelay
   vStpInsBridgeMaxAge
   vStpInsBridgeHelloTime
   vStpInsBridgeForwardDelay
   vStpInsCistRegionalRootId
   vStpInsCistPathCost
```

show spantree msti

Displays Spanning Tree bridge information for a Multiple Spanning Tree Instance (MSTI).

show spantree msti [*msti_id***]**

Syntax Definitions

msti_id	An existing MSTI ID number.

Defaults

By default, displays information for all MSTIs.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If an *msti_id* number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all MSTIs.
- This command displays Spanning Tree bridge information for an MSTI regardless of which mode (per-VLAN or flat) is active for the switch.
- Note that minimal information is displayed when this command is used in the per-VLAN mode, as MSTIs are not active in this mode. In addition, this command fails if MSTP is not the selected flat mode protocol.
- Note that MSTI 0 also represents the CIST instance that is always present on the switch. To view the CIST instance using this command, specify zero (0) for the *msti_id* number.

Examples

```
-> spantree mode flat
-> spantree protocol mstp
-> show spantree msti
  Spanning Tree Path Cost Mode : AUTO
 Msti STP Status Protocol Priority (Prio:SysID)
-----+----------+--------+--------------------
    0      ON      MSTP   32768 (0x8000:0x0000)
    1      ON      MSTP   32769 (0x8000:0x0001)

-> show spantree msti 0
Spanning Tree Parameters for Cist
  Spanning Tree Status :                   ON,
  Protocol             :   IEEE Multiple STP,
  mode                 :   FLAT (Single STP),
  Auto-Vlan-Containment:           Enabled   ,
  Priority             :        8192 (0x2000),
  Bridge ID            :   2000-e8:e7:32:8c:20:09,
  CST Designated Root  :   2000-e8:e7:32:8c:20:09,
  Cost to CST Root     :                    0,
  Designated Root      :   2000-e8:e7:32:8c:20:09,
```

```
  Cost to Root Bridge  :                    0,
  Root Port            :                 None,
  TxHoldCount          :                    3,
  Topology Changes     :                  203,
  Topology age         :              00:00:48,
  Last TC Rcvd Port    :                 2/1/2,
  Last TC Rcvd Bridge  :   3000-e8:e7:32:b9:24:13,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2

-> spantree mode per-vlan
-> show spantree msti
  Spanning Tree Path Cost Mode : AUTO
 ** Inactive flat mode instances: **
 Msti STP Status Protocol Priority (Prio:SysID)
-----+----------+--------+--------------------
    0      ON      MSTP   32768 (0x8000:0x0000)
    1      ON      MSTP   32769 (0x8000:0x0001)

-> show spantree msti 0
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters for Cist
  Spanning Tree Status :                ON,
  Protocol             :       IEEE Multiple STP,
  Priority             :    32768 (0x8000),
  TxHoldCount          :                 3,
  System Max Age (seconds)       =      20,
  System Forward Delay (seconds) =      15,
  System Hello Time (seconds)    =       2

-> show spantree msti 1
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters for Cist 1
  Spanning Tree Status :                ON,
  Protocol             :       IEEE Multiple STP,
  Priority             :    32769 (0x8001),
  TxHoldCount          :                 3,
  System Max Age (seconds)       =      20,
  System Forward Delay (seconds) =      15,
  System Hello Time (seconds)    =       2
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **spantree path-cost-mode** command.
Msti	The Multiple Spanning Tree Instance (MSTI) number. MSTI 0 represents the CIST. Configured through the **spantree msti** command.
STP Status	The Spanning Tree state for the instance (**ON** or **OFF**).

output definitions (continued)

Protocol	The Spanning Tree protocol applied to the instance (**STP, RSTP,** or **MSTP**). This value is not configurable for an MSTI. Configured through the **spantree protocol** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **spantree priority** command.
Spanning Tree Status	The Spanning Tree state for the instance (**ON** or **OFF**).
Mode	The Spanning Tree operating mode for the switch (**per-vlan** or **flat**). Configured through the **spantree mode** command.
Auto-Vlan-Containment	The auto VLAN containment status for the instance (**Enabled** or **Disabled**). AVC prevents a port that has no VLANs mapped to a Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Configured through the **spantree auto-vlan-containment** command.
Bridge ID	The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.
CST Designated Root	The bridge identifier for the root of the flat mode CIST instance. This field only appears when MSTP is active on the switch.
Cost to CST Root	The cost of the path to the root for the flat mode CIST instance. This field only appears when MSTP is active on the switch.
Designated Root	The bridge identifier for the root of the Spanning Tree for this instance.
Cost to Root Bridge	The cost of the path to the root for this Spanning Tree instance.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
TxHoldCount	The count to limit the transmission of BPDU through the port.
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.
Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (**hh:mm:ss** or **dd days and hh:mm:ss**).
Last TC Rcvd Port	The port that received the TC Flag Set in RSTP or MSTP protocol BPDU. Default value is None.
Last TC Rcvd Bridge	The adjacent designated bridge ID received from TC Flag Set in RSTP or MSTP BPDU along with Last TC Rcvd Port. This information is provided only for active RSTP and MSTP topologies. Default value is None.
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. MSTIs inherit this value from the CIST instance.
Forward Delay	The amount of time (in seconds) that a port remains in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. MSTIs inherit this value from the CIST instance.

output definitions (continued)

Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. MSTIs inherit this value from the CIST instance.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Hello Time	The Hello Time value for the root bridge.
BPDU Switching Enabled	The status of BPDU switching for the instance. This field only appears when BPDU switching is enabled. Configured through the **spantree bpdu-switching** command.

Release History

Release 7.1.1; command introduced.
Release 8.4.1; **Topology Change Port** field added.
Release 8.5R4; **Last TC Rcvd Bridge** field added.

Related Commands

show spantree	Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.
show spantree cist	Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree vlan	Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsProtocolSpecification
   vStpInsPriority
   vStpInsBridgeAddress
   vStpInsTimeSinceTopologyChange
   vStpInsTopChanges
   vStpInsDesignatedRoot
   vStpInsRootCost
   vStpInsRootPortNumber
   vStpInsNextBestRootCost
   vStpInsNextBestRootPortNumber
   vStpInsMaxAge
   vStpInsHelloTime
   vStpInsBridgeTxHoldCount
   vStpInsForwardDelay
   vStpInsBridgeMaxAge
   vStpInsBridgeHelloTime
   vStpInsBridgeForwardDelay
   vStpInsCistRegionalRootId
   vStpInsCistPathCost
   vStpInsMstiNumber
```

show spantree vlan

Displays Spanning Tree bridge information for a per-VLAN mode VLAN instance.

show spantree vlan [*vlan_id***]**

Syntax Definitions

vlan_id	An existing VLAN ID number.

Defaults

By default, displays information for all VLAN instances.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a *vlan_id* number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all VLAN instances.
- Specify a *vlan_id* number with this command to display Spanning Tree bridge information for a specific VLAN instance.
- This command displays Spanning Tree bridge information for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch. Note that minimal information is displayed when this command is used in the flat mode, as VLAN instances are not active in this mode.

Examples

```
-> spantree mode per-vlan
-> show spantree vlan
 Spanning Tree Path Cost Mode : AUTO
Vlan STP Status Protocol Priority
----+----------+--------+--------------
   1      ON       RSTP   32768 (0x8000)
 200      ON       RSTP   32768 (0x8000)
 500     OFF       RSTP   32768 (0x8000)
4094     OFF       RSTP   32768 (0x8000)

-> show spantree vlan 200
Spanning Tree Parameters for Vlan 200
  Spanning Tree Status :                   ON,
  Protocol             :       IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :         100 (0x0064),
  Bridge ID            :   0064-e8:e7:32:8c:20:09,
  Designated Root      :   0064-e8:e7:32:8c:20:09,
  Cost to Root Bridge  :                     0,
  Root Port            :                 None,
  TxHoldCount          :                    3,
  Topology Changes     :                    6,
  Topology age         :             00:00:04,
```

```
  Last TC Rcvd Port    :               2/1/2,
  Last TC Rcvd Bridge  :   012C-e8:e7:32:b9:24:13,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2

-> spantree mode flat
-> show spantree vlan 200
Single/Multiple Spanning Tree is enforced !! (flat mode)
INACTIVE Spanning Tree Parameters for Vlan 200
  Spanning Tree Status :               ON,
  Protocol             :       IEEE Rapid STP,
  Priority             :    32768 (0x8000),
  TxHoldCount          :                3,
  System Max Age (seconds)       =      20,
  System Forward Delay (seconds) =      15,
  System Hello Time (seconds)    =       2
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **spantree path-cost-mode** command.
Vlan	The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the **vlan** commands
STP Status	The Spanning Tree state for the instance (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to the VLAN instance (**STP** or **RSTP**). Note that MSTP is not supported for a VLAN instance. Configured through the **spantree protocol** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **spantree priority** command.
Spanning Tree Status	The Spanning Tree state for the instance (**ON** or **OFF**).
Mode	The Spanning Tree operating mode for the switch (**per-vlan** or **flat**). Configured through the **spantree mode** command.
Bridge ID	The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.
Designated Root	The bridge identifier for the root of the Spanning Tree for this instance.
Cost to Root Bridge	The cost of the path to the root for this Spanning Tree instance.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
Tx Hold Count	The count to limit the transmission of BPDU through the port.
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.

output definitions (continued)

Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (**hh:mm:ss** or **dd days and hh:mm:ss**).
Last TC Rcvd Port	The port that received the TC Flag Set in RSTP or MSTP protocol BPDU. Default value is None.
Last TC Rcvd Bridge	The adjacent designated bridge ID received from TC Flag Set in RSTP or MSTP BPDU along with Last TC Rcvd Port. This information is provided only for active RSTP and MSTP topologies. Default value is None.
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the **spantree max-age** command.
Forward Delay	The amount of time (in seconds) that a port remains in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **spantree forward-delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **spantree hello-time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Hello Time	The Hello Time value for the root bridge.
BPDU Switching Enabled	The status of BPDU switching for the instance. This field only appears when BPDU switching is enabled. Configured through the **spantree bpdu-switching** command.

Release History

Release 7.1.1; command introduced.
Release 8.4.1; **Topology Change Port** field added.
Release 8.5R4; **Last TC Rcvd Bridge** field added.

Related Commands

show spantree	Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.
show spantree cist	Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree msti	Displays the Spanning Tree bridge information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.

MIB Objects

vStpInsTable
- vStpInsNumber
- vStpInsMode
- vStpInsProtocolSpecification
- vStpInsPriority
- vStpInsBridgeAddress
- vStpInsTimeSinceTopologyChange
- vStpInsTopChanges
- vStpInsDesignatedRoot
- vStpInsRootCost
- vStpInsRootPortNumber
- vStpInsNextBestRootCost
- vStpInsNextBestRootPortNumber
- vStpInsMaxAge
- vStpInsHelloTime
- vStpInsBridgeTxHoldCount
- vStpInsForwardDelay
- vStpInsBridgeMaxAge
- vStpInsBridgeHelloTime
- vStpInsBridgeForwardDelay

show spantree ports

Displays Spanning Tree port information.

show spantree ports [forwarding | blocking | active | configured]

Syntax Definitions

forwarding	Displays Spanning Tree operational port parameters for ports that are forwarding for the specified instance.
blocking	Displays Spanning Tree operational port parameters for ports that are blocked for the specified instance.
active	Displays a list of active ports associated with the specified instance.
configured	Displays Spanning Tree administrative port parameters for all ports associated with the specified instance.

Defaults

parameter	default
forwarding | blocking | active | configured	all ports

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the switch is operating in the per-VLAN mode, this command displays port information for the VLAN instances.
- If the switch is operating in the flat mode and the protocol is STP or RSTP, this command displays port information for the single flat mode instance.
- If the switch is operating in the flat mode and the protocol is set to MSTP, this command displays port information for the MSTIs, including MSTI 0 (also known as the CIST).

Examples

```
-> spantree mode flat
-> spantree protocol rstp
-> show spantree ports

 Brdge  Port  Oper Status  Path Cost  Role   loop-guard   Note
------+------+------------+---------+------+-----------+-----
    1  1/3        DIS             0    DIS         DIS
    1  1/4        DIS             0    DIS         DIS
    1  1/6        DIS             0    DIS         DIS
    1  1/7        DIS             0    DIS         DIS
    1  1/9        DIS             0    DIS         DIS
```

```
    1  1/10       DIS             0    DIS         DIS
    1  0/1        BLK             0    ALT         ENA   ERR

-> spantree protocol mstp
-> show spantree ports
 Msti  Port  Oper Status  Path Cost  Role    loop-guard   Note
------+------+------------+---------+-------+-----------+-----
    1  1/3        DIS             0    DIS         DIS
    1  1/4        DIS             0    DIS         DIS
    1  1/6        DIS             0    DIS         DIS
    1  1/7        DIS             0    DIS         DIS
    1  1/9        DIS             0    DIS         DIS
    1  1/10       DIS             0    DIS         DIS
    1  0/1        BLK             0    ALT         ENA    ERR
   10  1/1       FORW            19   DESG         ENA

-> spantree mode per-vlan
-> show spantree ports

 Vlan  Port Oper Status  Path Cost  Role    loop-guard   Notes
-----+-----+------------+---------+-------+-----------+--------
    1  1/1/1       DIS           0    DIS         DIS
    1  1/1/2       DIS           0    DIS         DIS
    1  1/1/3       DIS           0    DIS         DIS
    1  1/1/4       DIS           0    DIS         DIS
    1  1/1/5       DIS           0    DIS         DIS
    1  1/1/6       DIS           0    DIS         DIS

-> show spantree ports active
 Brdge  Port  Oper Status  Path Cost  Role   loop-guard   Note
-----+------+------------+---------+-------+-----------+-------
   10  2/1       FORW            19   DESG         ENA
  172  2/8       FORW            19   ROOT         DIS
 1001  2/1       FORW            19   DESG         DIS

-> show spantree ports blocking
 Brdge  Port  Oper Status  Path Cost  Role   loop-guard   Note
------+------+------------+---------+-------+-----------+-------
   1   0/1        BLK             19   DESG         ENA   ERR
  172  2/8        BLK             29   ALT          DIS
```

output definitions

Bridge, Msti, or Vlan	The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol in the flat mode. The MSTI number when MSTP is the active protocol in the flat mode. The VLAN ID number when STP or RSTP is the active protocol in the per-VLAN mode.
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Oper Status	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, learning, and forwarding.

output definitions (continued)

Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **spantree msti path-cost** or **spantree vlan path-cost**command.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.
loop-guard	Displays if the loop-guard is enabled (ENA) or disabled (DIS) on the port. Configured through the **spantree loop-guard** command.
Note	Displays a note if the port has entered the error violation state (ERR); then the port role of the port instance in that row becomes insignificant.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree cist ports	Displays Spanning Tree port information for the flat mode CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.
show spantree msti ports	Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.
show spantree vlan ports	Displays Spanning Tree port information for VLAN instances when the switch is operating in the per-VLAN or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortEnable
   vStpInsPortState
   vStpInsPortManualMode
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortRole
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
   vStpInsPortAdminEdge
   vStpInsPortAutoEdge
   vStpInsPortRestrictedRole
   vStpInsPortRestrictedTcn
   vStpInsPortPrimaryPortNumber
   vStpInsPortDesignatedRoot
   vStpInsPortDesignatedBridge
   vStpPortConfigPVST
   vStpPortConfigStatePVST
   vStpBridgeModePVST
```

show spantree cist ports

Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist ports [forwarding | blocking | active | configured]

Syntax Definitions

forwarding	Displays Spanning Tree operational port parameters for ports that are forwarding for the CIST instance.
blocking	Displays Spanning Tree operational port parameters for ports that are blocked for the CIST instance.
active	Displays a list of active ports associated with the CIST instance.
configured	Displays Spanning Tree administrative port parameters for the CIST instance.

Defaults

parameter	default
forwarding | blocking | active | configured	all ports

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command displays Spanning Tree port information for the flat mode CIST instance regardless of which mode (per-VLAN or flat) is active for the switch.
- Note that minimal information is displayed when this command is used in the per-VLAN mode, as the CIST is not active in this mode.

Examples

```
-> show spantree cist ports

Spanning Tree Port Summary for Cist
      Oper  Path   Desig        Prim. Op Op
Port   St   Cost    Cost   Role Port Cnx Edg   Desig Bridge ID         Note
-----+----+-------+-------+----+----+---+----+----------------------+--------
 1/1  FORW  200000      52 ROOT 1/1  PTP  EDG  8000-00:30:f1:5b:37:73
 1/2   DIS       0       0  DIS 1/2   NS   No  0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS 1/3   NS  EDG  0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS 1/4   NS   No  0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS 1/5   NS  EDG  0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS 1/6   NS  EDG  0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS 1/7   NS  EDG  0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS 1/8   NS   No  0000-00:00:00:00:00:00
```

```
-> show spantree cist ports active

Spanning Tree Port Summary for Cist
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg  Desig Bridge ID         Note
-----+----+-------+-------+----+----+----+---+--------------------+---------
1/1  FORW  200000      52 ROOT  1/1  PTP  EDG  8000-00:30:f1:5b:37:73

-> show spantree cist ports

Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg  Desig Bridge ID        Note
-----+----+-------+-------+----+-----+---+---+--------------------+---------
 1/1   DIS       0       0  DIS  1/1   NS  NO 0000-00:00:00:00:00:00
 1/2   DIS       0       0  DIS  1/2   NS  NO 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS  1/3   NS  NO 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS  1/4   NS  NO 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS  1/5   NS  NO 0000-00:00:00:00:00:00
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **spantree vlan path-cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.
Prim. Port	The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
Op Cnx	Operational connection type: **PTP, NPT**, or **NS** (nonsignificant). Shows the current operational state of the port connection type. See the **spantree vlan connection** command for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port connection type. See the **spantree vlan connection** command for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port segment.

```
-> show spantree cist ports configured

Spanning Tree Port Admin Configuration for Vlan 1
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/   PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard  Cfg Stat
-----+----+----+----+-------+----+----+----+----+-----------+-----------
 1/1     7  ENA  No        0  AUT   No  Yes   No       No      AUT  Off
 1/2     7  ENA  No        0  NPT   No  Yes   No       No      AUT  Off
 1/3     7  ENA  No        0  NPT   No  Yes   No       No      AUT  Off
 1/4     7  ENA  No        0  NPT   No  Yes   No       No      AUT  Off
 1/5     7  ENA  No        0  NPT   No  Yes   No       No      AUT  O
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Port Pri	The Spanning Tree priority for the port. The lower the number, the higher the priority.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**.
Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **spantree vlan path-cost** command.
Config Cost	The configured path cost value for this port. Configured through the **spantree vlan path-cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT.** Configured through the **spantree vlan connection** command.
Adm Edg	The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port**.** Configured through the **spantree vlan connection** command.
Aut Edg	The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the **spantree cist auto-edge** or **spantree vlan auto-edge** command.
Rstr Tcn	The restricted TCN capability: **yes** indicates that the port supports the restricted TCN capability; **no** indicates that the port does not support the restricted TCN capability. Configured through the **spantree cist restricted-tcn** or **spantree vlan restricted-tcn** command.
Rstr Role	The restricted role port status: **yes** indicates that the port is a restricted role port; **no** indicates that the port is not a restricted role port. Configured through the **spantree cist restricted-role** or **spantree vlan restricted-role** command.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree ports	Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.
show spantree msti ports	Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortState
   vStpInsPortEnable
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortDesignatedBridge
   vStpInsPortAdminEdge
   vStpInsPortAutoEdge
   vStpInsPortRestrictedRole
   vStpInsPortRestrictedTcn
   vStpInsPortManualMode
   vStpInsPortRole
   vStpInsPrimaryPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

show spantree msti ports

Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).

show spantree msti [*msti_id***] ports [forwarding | blocking | active | configured]**

Syntax Definitions

msti_id	An existing MSTI ID number.
forwarding	Displays Spanning Tree operational port parameters for ports that are forwarding for the MSTI instance.
blocking	Displays Spanning Tree operational port parameters for ports that are blocked for the MSTI instance.
active	Displays a list of active ports associated with the MSTI instance.
configured	Displays Spanning Tree administrative port parameters for the MSTI instance.

Defaults

parameter	default
msti_id	all MSTIs
forwarding | blocking | active | configured	all ports

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If an *msti_id* number is *not* specified, this command displays the Spanning Tree port operational status, path cost, and role values for all associated MSTIs.
- This command displays Spanning Tree port information for an MSTI regardless of which mode (per-VLAN or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the per-VLAN mode, as MSTIs are not active in this mode. In addition, if MSTP is not the selected flat mode protocol, this command fails.
- The **configured** keyword is only available when an instance number is specified with this command. In addition, this keyword cannot be used in combination with either the **forwarding** or **blocking** keywords.
- Note that MSTI 0 also represents the CIST instance that is always present on the switch. To view the CIST instance using this command, specify zero (0) for the *msti_id* number.

Examples

```
-> show spantree msti ports
 Msti  Port Oper Status  Path Cost  Role
-----+-----+------------+---------+-----
    0  1/1      FORW       200000   ROOT
    0  1/2       DIS           0    DIS
    0  1/3       DIS           0    DIS
    0  1/4       DIS           0    DIS
    0  1/5       DIS           0    DIS
    0  1/6       DIS           0    DIS
    0  1/7       DIS           0    DIS
    0  1/8       DIS           0    DIS
    0  1/9       DIS           0    DIS
    0  1/10      DIS           0    DIS
    0  1/11      DIS           0    DIS
    0  1/12      DIS           0    DIS
    0  1/13      DIS           0    DIS
    0  1/14      DIS           0    DIS
    0  1/15      DIS           0    DIS
    0  1/16      DIS           0    DIS
    0  1/17      DIS           0    DIS
    0  1/18      DIS           0    DIS
    0  1/19      DIS           0    DIS
    0  1/20      DIS           0    DIS
    0  1/21      DIS           0    DIS
    0  1/22      DIS           0    DIS
    0  1/23      DIS           0    DIS
    0  1/24      DIS           0    DIS
    0  5/1       DIS           0    DIS
    0  5/2       DIS           0    DIS
    1  1/1      FORW       200000   MSTR
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12      DIS           0    DIS
    1  1/13      DIS           0    DIS
    1  1/14      DIS           0    DIS
    1  1/15      DIS           0    DIS
    1  1/16      DIS           0    DIS
    1  1/17      DIS           0    DIS
    1  1/18      DIS           0    DIS
    1  1/19      DIS           0    DIS
    1  1/20      DIS           0    DIS
    1  1/21      DIS           0    DIS
    1  1/22      DIS           0    DIS
    1  1/23      DIS           0    DIS
    1  1/24      DIS           0    DIS
    1  5/1       DIS           0    DIS
    1  5/2       DIS           0    DIS
```

```
-> show spantree msti 0 ports

Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg  Desig Bridge ID        Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
 1/1   DIS       0       0  DIS  1/1   NS  NO 0000-00:00:00:00:00:00
 1/2   DIS       0       0  DIS  1/2   NS  NO 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS  1/3   NS  NO 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS  1/4   NS  NO 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS  1/5   NS  NO 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS  1/6   NS  NO 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS  1/7   NS  NO 0000-00:00:00:00:00:00

-> show spantree msti 0 ports configured

Spanning Tree Port Admin Configuration for Vlan 1
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/   PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn   Root Guard  Cfg Stat
-----+----+----+----+-------+----+----+----+----+-----------+-----------
 1/1     7  ENA  No        0  AUT   No  Yes   No       No      AUT  Off
 1/2     7  ENA  No        0  NPT   No  Yes   No       No      AUT  Off
 1/3     7  ENA  No        0  NPT   No  Yes   No       No      AUT  Off
 1/4     7  ENA  No        0  NPT   No  Yes   No       No      AUT  Off
 1/5     7  ENA  No        0  NPT   No  Yes   No       No      AUT
```

output definitions

Msti	The Multiple Spanning Tree Instance (MSTI) number. MSTI 0 represents the CIST. Configured through the **spantree msti** command.
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **spantree msti path-cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
RSTR Role/ Root Guard	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
Prim. Port	The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
Op Cnx	Operational connection type: **PTP, NPT**, or **NS** (nonsignificant). Shows the current operational state of the port connection type. See the **spantree vlan connection** command for more information.

output definitions (continued)

Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port connection type. See the **spantree vlan connection** command for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port segment.
PVST+ Cfg	Indicates the current PVST+ port configuration (**auto**, **enable** or **disable**).
PVST+ Stat	Indicates the current status of the PVST+ mode (**On** or **Off**).

```
-> show spantree msti 2 ports configured
Spanning Tree Port Admin Configuration for Msti 2
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  Opt.
-----+----+----+----+-------+----+----+----+----+----------+--------
 1/1     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/2     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/3     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/4     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/5     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/6     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/7     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/8     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/9     7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/10    7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/11    7  ENA  No        0  AUT   No  Yes   No   No        DIS
 1/12    7  ENA  No        0  AUT   No  Yes   No   No        DIS
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Port Pri	The Spanning Tree priority for the port. It is a numeric value and the lower the number, the higher the priority. Configured through the **spantree priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** - ENA or **disabled -** DIS.
Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **spantree vlan path-cost** command.
Config Cost	The configured path cost value for this port. Configured through the **spantree msti path-cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT.** Configured through the **spantree vlan connection** command.
Adm Edg	The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port**.** Configured through the **spantree vlan connection** command.

output definitions (continued)

Aut Edg	The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the **spantree cist auto-edge** or **spantree vlan auto-edge** command.
Rstr Tcn	The restricted TCN capability: **yes** indicates that the port supports the restricted TCN capability; **no** indicates that the port does not support the restricted TCN capability. Configured through the **spantree cist restricted-tcn** or **spantree vlan restricted-tcn** command.
Rstr Role	The restricted role port status: **yes** indicates that the port is a restricted role port; **no** indicates that the port is not a restricted role port. Configured through the **spantree cist restricted-role** or **spantree vlan restricted-role** command.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree ports	Displays Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.
show spantree cist ports	Displays Spanning Tree port information for a CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.
show spantree vlan ports	Displays Spanning Tree port information for a VLAN when the switch is operating in the per-VLAN or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortState
   vStpInsPortEnable
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortDesignatedBridge
   vStpInsPortAdminEdge
   vStpInsPortAutoEdge
   vStpInsPortRestrictedRole
   vStpInsPortRestrictedTcn
   vStpInsPortManualMode
   vStpInsPortRole
   vStpPortConfigPVST
   vStpPortConfigStatePVST
   vStpBridgeModePVST
   vStpInsPrimaryPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

show spantree vlan ports

Displays Spanning Tree port information for a VLAN instance.

show spantree vlan [*vlan_id***[-***vlan_id2***]] ports [forwarding | blocking | active | configured]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	An existing VLAN ID number. Use a hyphen to specify a range of VLAN IDs (for example, **vlan 10-15**).
forwarding	Displays Spanning Tree operational port parameters for ports that are forwarding for the VLAN instance.
blocking	Displays Spanning Tree operational port parameters for ports that are blocked for the VLAN instance.
active	Displays a list of active ports associated with the VLAN instance.
configured	Displays Spanning Tree administrative port parameters for the VLAN instance.

Defaults

parameter	default
vlan_id	all VLAN instances
forwarding | blocking | active | configured	all ports

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a *vlan_id* number is *not* specified, this command displays the Spanning Tree port operational status, path cost, and role values for all VLAN instances.
- Specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (e.g., **show spantree vlan 10-15 ports**). Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs— is allowed with this command. Multiple entries are not accepted.
- This command displays Spanning Tree port information for a VLAN instance regardless of which mode (per-VLAN or flat) is active for the switch.
- Note that minimal information is displayed when this command is used in the flat mode, as VLAN instances are not active in this mode.
- The **configured** keyword is only available when a VLAN ID is specified with this command. In addition, this keyword cannot be used in combination with either the **forwarding** or **blocking** keywords.

Examples

```
-> show spantree vlan ports
 Vlan  Port Oper Status  Path Cost  Role    Note
-----+-----+------------+---------+-------+---------
    1  1/1       DIS           0    DIS
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12     FORW          19    DIS


-> show spantree vlan 1 ports
Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
 1/1   DIS       0       0  DIS  1/1   NS EDG 0000-00:00:00:00:00:00
 1/2   DIS       0       0  DIS  1/2   NS  NO 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS  1/3   NS  NO 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS  1/4   NS  NO 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS  1/5   NS  NO 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS  1/6   NS  NO 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS  1/7   NS  NO 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS  1/8   NS  NO 0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS  1/9   NS  NO 0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS  1/10  NS  NO 0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS  1/11  NS  NO 0000-00:00:00:00:00:00
 1/12 FORW      19       0  DIS  1/12 PTP  NO 0001-00:d0:95:6a:79:50


-> show spantree vlan 1 ports active
Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
 1/12 FORW      19       0  DIS 1/12 PTP EDG 0001-00:d0:95:6a:79:50


-> show spantree vlan 10-13 ports
Spanning Tree Port Summary for Vlan 10
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
 1/46  DIS       0       0  DIS 1/46  NS  EDG 0000-00:00:00:00:00:00
Spanning Tree Port Summary for Vlan 11
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
 1/36  DIS       0       0  DIS 1/36  NS EDG 0000-00:00:00:00:00:00
 1/37  DIS       0       0  DIS 1/37  NS  NO 0000-00:00:00:00:00:00
```

```
Spanning Tree Port Summary for Vlan 12
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
 1/42  DIS       0       0  DIS 1/42  NS  EDG 0000-00:00:00:00:00:00
 1/43  DIS       0       0  DIS 1/43  NS   NO 0000-00:00:00:00:00:00
Spanning Tree Port Summary for Vlan 13
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
 1/38  DIS       0       0  DIS 1/38  NS  EDG 0000-00:00:00:00:00:00
```

output definitions

Vlan	The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the **vlan** commands
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **spantree vlan path-cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
Prim. Port	The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
Op Cnx	Operational connection type: **PTP, NPT**, or **NS** (nonsignificant). Shows the current operational state of the port's connection type. See the **spantree vlan connection** command for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port's connection type. See the **spantree vlan connection** command for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree vlan 1 ports configured
Spanning Tree Port Admin Configuration for Vlan 1
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/  PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+----------
 1/1     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/2     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/3     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/4     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/5     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/6     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/7     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/8     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/9     7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/10    7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/11    7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/12    7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF

-> show spantree vlan 10-13 ports configured
Spanning Tree Port Admin Configuration for Vlan 10
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/  PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+----------
 1/46    7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
Spanning Tree Port Admin Configuration for Vlan 11
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/  PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+----------
 1/36    7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
 1/37    7  ENA  No        0  AUT   No  Yes   No    No       AUT OFF
Spanning Tree Port Admin Configuration for Vlan 12
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/  PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+----------
 1/42    7  ENA  No        0  AUT   No  Yes  No     No       AUT OFF
 1/43    7  ENA  No        0  AUT   No  Yes  No     No       AUT OFF
Spanning Tree Port Admin Configuration for Vlan 13
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/  PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+----------
 1/38    7  ENA  No        0  AUT   No  Yes  No     No       AUT OFF
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **spantree priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **spantree vlan** command to enable or disable Spanning Tree on a port.

output definitions (continued)

Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **spantree loop-guard** command.
Config Cost	The configured path cost value for this port. Configured through the **spantree vlan path-cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT**. Configured through the **spantree vlan path-cost** command.
Adm Edg	The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port**.** Configured through the **spantree vlan connection** command.
Aut Edg	The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the **spantree cist auto-edge** or **spantree vlan auto-edge** command.
Rstr Tcn	The restricted TCN capability: **yes** indicates that the port supports the restricted TCN capability; **no** indicates that the port does not support the restricted TCN capability. Configured through the **spantree cist restricted-tcn** or **spantree vlan restricted-tcn** command.
Rstr Role/Root Guard	The restricted status of the port: **Yes** indicates that the port is restricted from becoming the root; **No** indicates that the port is not restricted from becoming the root. Configured through the **spantree cist restricted-role** or **spantree vlan restricted-role** command.
PVST+ Cfg	The type of BPDU used on the port: **AUTO** indicates that IEEE BPDUs are used until a PVST+ BPDU is detected; **ENA** indicates that PVST+ BPDUs are used; **DIS** indicates that IEEE BPDUs are used. Configured through the **spantree pvst+compatibility** command.
PVST+ Stat	Indicates whether or not the PVST+ interoperability status is enabled (**ENA**) or disabled (**DIS**) for the port. Configured through the **spantree pvst+compatibility** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show spantree ports	Displays Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.
show spantree cist ports	Displays Spanning Tree port information for a CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.
show spantree msti ports	Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortState
   vStpInsPortEnable
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortDesignatedBridge
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
   vStpInsPortAdminEdge
   vStpInsPortAutoEdge
   vStpInsPortRestrictedRole
   vStpInsPortRestrictedTcn
   vStpInsPortManualMode
   vStpInsPortRole
   vStpInsPrimaryPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

show spantree mode

Displays the current global Spanning Tree mode parameter values for the switch.

show spantree mode

Syntax Definition

N/A

Defaults

NA

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The global parameters for spanning tree can be activated or configured using the related commands.

Examples

```
-> show spantree mode

Spanning Tree Global Parameters
  Current Running Mode  : Per VLAN,
  Current Protocol      : N/A (Per VLAN),
  Path Cost Mode        : 32 BIT,
  Auto Vlan Containment : N/A
  Cisco PVST+ mode      : Disabled
Vlan Consistency check   : Disabled
```

output definitions

Current Running Mode	The spantree mode active on the switch. (**Flat** or **Per VLAN**)
Current Protocol	The spantree protocol active on the switch.
Path Cost Mode	The path cost mode value configured on the switch. (**AUTO** or **32 BIT**)
Auto Vlan Containment	The Auto VLAN containment mode configured on the switch (**Enabled** or **Disabled**).
Cisco PVST+ mode	The PVST+ mode configured on the switch (**Enabled** or **Disabled**).
Vlan Consistency check	Specifies if VLAN consistency check is **Enabled** or **Disabled** on the switch.

Related Commands

spantree mode	Assigns a flat Spanning Tree or per-VLAN Spanning Tree operating mode for the switch.
spantree protocol	Configures the Spanning Tree protocol for the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance if the switch is running in the per-VLAN mode.
spantree path-cost-mode	Configures the automatic selection of a 16-bit path cost for STP/RSTP ports and a 32-bit path cost for MSTP ports or sets all path costs to use a 32-bit value.
spantree pvst+compatibility	Enables or disables PVST+ mode on the switch, port or link aggregate enabling them to operate with Cisco switches.
spantree auto-vlan-containment	Enables or disables Auto VLAN Containment (AVC).

Release History

Release 7.1.1; command introduced.

MIB Objects

```
vStpTable
   vStpMode
vStpInsTable
   vStpInsProtocolSpecification
vStpBridge
   vStpPathCostMode
vStpMstRegionTable
   vStpBridgeModePVST
vStpBridge
   vStpBridgeAutoVlanContainment
```

show spantree mst

Displays the Multiple Spanning Tree (MST) information for a MST region or the specified port or link aggregate on the switch.

show spantree mst {region | port *chassis/slot/port* | **linkagg** *agg_id***}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number and port number of the physical port.
*agg_id***[**-*agg_id2***]**	The link aggregate ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Three MST region attributes (configuration name, revision level, and configuration digest) define an MST region as required by the IEEE 802.1Q 2005 standard. Switches that share the same values for these attributes are all considered part of the same region. Currently each switch can belong to one MST region at a time.
- This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.
- Specify the port number or link aggregate ID along with the **port** or **linkagg** keyword to get information related to the specified port or link aggregate.

Examples

```
-> show spantree mst region

Configuration Name   = Region 1
Revision Level       = 0
Configuration Digest = 0xac36177f 50283cd4 b83821d8 ab26de62
Revision Max hops    = 20
Cist Instance Number = 0

-> show spantree mst port 1/2

MST  Role  State Pth Cst  Edge Boundary Op Cnx Vlans
---+------+-----+--------+----+--------+------+---------------
  0   DIS    DIS        0   NO    YES     NS    1
 12   DIS    DIS        0   NO    YES     NS
```

```
-> show spantree mst linkagg 4

MST  Role  State Pth Cst  Edge Boundary Op Cnx Vlans
---+------+-----+--------+----+--------+------+--------------
  0  DESG   FORW     6000   NO    NO     NS    1
  1  DESG   FORW        0   NO    NO     NS
  2  DESG   FORW        0   NO    NO     NS
```

output definitions

Configuration Name	An alphanumeric string that identifies the name of the MST region. Use the **spantree mst region name** command to define this value.
Revision Level	A numeric value that identifies the MST region revision level for the switch.
Configuration Digest	An MST region identifier consisting of a 16 octet hex value (as per the IEEE 802.1Q 2005 standard) that represents all defined MSTIs and their associated VLAN ranges. Use the **spantree msti** and **spantree msti vlan** commands to define VLAN to MSTI associations.
Revision Max hops	The number of maximum hops authorized for region information. Configured through the **spantree mst region max-hops** command.
Cist Instance Number	The number of the CIST instance, which is currently zero as there is only one region per switch. Therefore, only one CIST exists per switch Note that this instance is also known as the flat mode instance and is known as bridge 1 when using STP or RSTP.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigDigest
   vStpMstRegionConfigName
   vStpMstRegionConfigRevisionLevel
   vStpMstRegionCistInstanceNumber
   vStpMstRegionMaxHops
```

show spantree msti vlan-map

Displays the range of VLANs associated with the specified Multiple Spanning Tree Instance (MSTI).

show spantree msti [*msti_id***] vlan-map**

Syntax Definitions

msti_id	An existing MSTI ID number.

Defaults

By default, the VLAN to MSTI mapping is displayed for all MSTIs.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If an *msti_id* is not specified, then the VLAN to MSTI mapping for all defined MSTIs is displayed.
- This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance.

Examples

```
-> show spantree msti vlan-map

 Cist
 Name                :
 VLAN list           : 1-9,14-4094

 Msti 1
 Name                :
 VLAN list           : 10-11

 Msti 2
 Name                :
 VLAN list           : 12-13

-> show spantree msti 2 vlan-map

 Msti 2
 Name                : MS1,
 VLAN list           : 12-13
```

output definitions

Cist Instance	Identifies MSTI VLAN mapping information for the CIST instance.
Msti	The MSTI ID number that identifies an association between a Spanning Tree instance and a range of VLANs.

output definitions (continued)

Name	An alphanumeric value that identifies an MSTI name. Use the **spantree msti** command to define an MSTI name.
VLAN list	The range of VLAN IDs that are associated with this MSTI.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree mst	Displays the MST region information for the switch.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapState
```

show spantree cist vlan-map

Displays the range of VLANs associated with the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist vlan-map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.

Examples

```
-> show spantree cist vlan-map

 Cist
 Name           : CIST1,
 VLAN list      : 1-9,14-4094
```

output definitions

Name	An alphanumeric value that identifies the name of the CIST. Use the **spantree msti** command to define a name for this instance.
VLAN list	The range of VLAN IDs that are associated with the CIST instance.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree mst	Displays the MST region information for the switch.
show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapState
```

show spantree map-msti

Displays the Multiple Spanning Tree Instance (MSTI) that is associated to the specified VLAN.

show spantree [vlan *vlan_id***] map-msti**

Syntax Definitions

vlan_id	An existing VLAN ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance.

Examples

```
-> show spantree map-msti

 Vlan   Msti/Cist(0)
------+--------------------------
   200    1
```

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree mst	Displays the MST region information for the switch.
show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.

MIB Objects

```
vStpMstVlanAssignmentTable
   vStpMstVlanAssignmentVlanNumber
   vStpMstVlanAssignmentMstiNumber
```

9 Shortest Path Bridging Commands

The OmniSwitch supports Shortest Path Bridging MAC (SPBM), as defined in the IEEE 802.1aq standard. SPB-M uses the Provider Backbone Bridge (PBB) network model to encapsulate (using IEEE 802.1ah headers) and tunnel customer traffic through the network backbone. The shortest path trees (SPTs) upon which the PBB network infrastructure operates are determined using a version of the Intermediate System-to-Intermediate System (IS-IS) link state protocol that supports TLV extensions for SPB (ISIS-SPB).

The SPBM network topology consists of two layers: the backbone infrastructure (control plane) layer and the services (data plane) layer. ISIS-SPB builds the backbone layer by defining loop-free, SPTs through the backbone network. The service layer is based on the PBB framework as defined in the IEEE 802.1ah standard. SPBM supports the 802.1ah MAC-in-MAC method for data encapsulation. SPBM services transport the encapsulated traffic over the ISIS-SPB infrastructure.

This chapter documents the Command Line Interface (CLI) commands used to configure and verify the ISIS-SPB backbone. For commands used to configure and verify the SPBM services layer, see Chapter 10, “Service Manager Commands.”

MIB information for the SPB commands is as follows:

Filename: ALCATEL-IND1-ISIS-SPB-MIB.mib
Module: alcatelIND1IsisSpbMib

Filename: ALCATEL-IND1-VLAN-MGR-MIB.mib
Module: alcatelIND1VLANMgrMIB

A summary of the available commands is listed here:

Global SPB Commands	**spb isis admin-state** **spb isis area-address** **spb isis bridge-priority** **spb isis source-id** **spb isis control-address** **spb isis spf-wait** **spb isis lsp-wait** **spb isis rapid-lsp-converge** **spb isis overload** **spb isis overload-on-boot**
SPB Backbone VLAN (BVLAN) Commands	**spb bvlan** **spb isis bvlan ect-id** **spb isis control-bvlan** **spb isis bvlan tandem-multicast-mode**
SPB Interface Commands	**spb isis interface**

SPB IP VPN Commands	**spb ipvpn bind** **spb ipvpn redist** **show spb ipvpn bind** **show spb ipvpn redist** **show spb ipvpn route-table**
SPB IPv6 VPN Commands	**spb ipvpn6 bind** **spb ipvpn6 redist** **show spb ipvpn6 bind** **show spb ipvpn6 redist** **show spb ipvpn6 route-table**
SPB Graceful Restart Commands	**spb isis graceful-restart** **spb isis graceful-restart helper**
SPB Show Commands	**show spb isis info** **show spb isis bvlans** **show spb isis interface** **show spb isis adjacency** **show spb isis database** **show spb isis nodes** **show spb isis unicast-table** **show spb isis services** **show spb isis spf** **show spb isis multicast-table** **show spb isis multicast-sources** **show spb isis multicast-sources-spf** **show spb isis ingress-mac-filter** **show spb isis rapid-lsp-converge-info** **show spb isis rapid-lsp-converge-table**

spb bvlan

Configures an SPB backbone VLAN (BVLAN).

spb bvlan {*bvlan_id***[-***bvlan_id2***]} [admin-state {enable | disable}] [name** *description***]**

no spb bvlan *bvlan_id*

Syntax Definitions

*bvlan_id***[-***bvlan_id2***]**	A numeric value that uniquely identifies an individual BVLAN. The valid ID range is 1–4094. Use a hyphen to specify a range of BVLAN IDs (10-20).
enable	Enables the VLAN administrative status.
disable	Disables the VLAN administrative status.
description	An alphanumeric string. Optional name description for the VLAN ID.

Defaults

parameter	default
enable | disable	**enable**
description	**VLAN ID**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a BVLAN from the switch configuration. All BVLAN ports are detached before the BVLAN is removed.
- The description can be any alphanumeric string. Enclose the description in double quotes if it contains more than one word with a space in between.
- The BVLAN configuration must be the same on each SPB bridge to ensure proper ISIS-SPB neighbor discovery and shortest path calculations throughout the provider backbone bridge (PBB) network.
- BVLANs differ from standard VLANs as follows:
  - No Spanning Tree control—the Spanning Tree protocol is automatically disabled on each BVLAN, and all ports associated with each BVLAN will remain in a forwarding state. However, Spanning Tree can remain operational on other types of VLANs.
  - No source MAC address learning—normal hardware learning is disabled on BVLANs. Instead, the forwarding database (FDB) is populated by the ISIS-SPB protocol.
  - There is no flooding of unknown destination or multicast frames.
  - Ingress filtering based on the source MAC address—frames received on ports that do not have an incoming source MAC address pre-programmed by ISIS-SPB are discarded.
- All BVLANs are automatically associated with all ISIS-SPB interfaces. Adding or removing BVLANs from a specific SPB interface is not allowed.

- The maximum number of BVLANs supported is four.
- BVLANs and standard VLANs can co-exist on the same bridge ports.

Examples

```
-> spb bvlan 200 name BVLAN-200
-> spb bvlan 720 admin-state disable
-> spb bvlan 500 name BVLAN-500 admin-state enable
-> no spb bvlan 1020
```

Release History

Release 7.3.1; command introduced.

Related Commands

spb isis control-bvlan	Configures a control BVLAN
spb isis bvlan ect-id	Assigns an equal cost tree (ECT) algorithm ID to the specified BVLAN.
spb isis bvlan tandem-multicast-mode	Configures the tandem multicast mode for the specified SPB backbone VLAN (BVLAN).
spb isis interface	Configures ISIS-SPB network interfaces.
show spb isis bvlans	Displays the BVLAN configuration for the switch.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanType
```

spb isis bvlan ect-id

Configures the equal cost tree (ECT) identifier for the specified SPB backbone VLAN (BVLAN). The ECT ID assigns a tie-breaking algorithm to the BVLAN that is used for shortest path tree (SPT) calculations.

spb isis bvlan *bvlan_id* **ect-id** *ect_id*

Syntax Definitions

bvlan_id	An existing BVLAN ID.
ect_id	An ECT algorithm ID. The valid range is 1–16.

Defaults

By default, the next available ECT ID number is automatically assigned to a BVLAN when the BVLAN is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to change the existing ECT ID number for the specified BVLAN on each SPB brdige, as necessary, to make sure the specified BVLAN uses the same ECT ID throughout the network.
- The BVLAN ID specified with this command must already exist in the switch configuration.

Examples

```
-> spb isis bvlan 200 ect-id 5
-> spb isis bvlan 720 ect-id 10
```

Release History

Release 7.3.1; command introduced.

Related Commands

spb bvlan	Creates a SPB backbone VLAN (BVLAN).
show spb isis bvlans	Displays the SPB BVLAN configuration for the switch.

MIB Objects

```
alcatelIND1IsisSpbEctStaticTable
   alcatelIND1IsisSpbEctStaticEntryBaseVid
```

spb isis control-bvlan

Designates an existing BVLAN that will serve as the control BVLAN for the bridge. Only one BVLAN per bridge is designated as the control BVLAN, which is used to exchange ISIS-SPB control packets with neighboring SPB bridges on behalf of all the BVLANs configured for that bridge.

spb isis control-bvlan *bvlan_id*

Syntax Definitions

bvlan_id	An existing BVLAN ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The BVLAN ID specified with this command must already exist in the switch configuration.
- The control BVLAN ID is the VLAN tag that is applied to ISIS-SPB control frames.
- Configuring an existing BVLAN as the control BVLAN does not exclude that VLAN from carrying data traffic for the SPB domain. In other words, a single VLAN can serve as both a regular BVLAN and the control BVLAN at the same time.

Examples

```
-> spb isis control-bvlan 200
-> spb isis control-bvlan 720
```

Release History

Release 7.3.1; command introduced.

Related Commands

spb bvlan	Configures an SPB BVLAN.
show spb isis bvlans	Displays the BVLAN configuration for the bridge.

MIB Objects

```
alcatelIND1IsisSpbSys
   alcatelIND1IsisSpbSysControlBvlan
```

spb isis bvlan tandem-multicast-mode

Configures the tandem multicast mode for the specified SPB backbone VLAN (BVLAN). This mode is only applicable to associated SPB service instances that are configured to use the tandem replication mode for multicast traffic.

spb isis bvlan *bvlan_id* **tandem-multicast-mode {sgmode | gmode}**

Syntax Definitions

bvlan_id	An existing BVLAN ID.
sgmode	Specifies the source and group (S,G) mode for the BVLAN.
gmode	Specifies the any source and group (*,G).

Defaults

By default, BVLANs are configured to use the (S,G) mode.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The BVLAN ID specified with this command must already exist in the switch configuration.
- The (S,G) mode identifies a source-specific multicast distribution tree.
- The (*,G) mode identifies a shared multicast distribution tree.

Examples

```
-> spb isis bvlan 200 tandem-multicast-mode gmode
-> spb isis bvlan 720 tandem-multicast-mode sgmode
```

Release History

Release 7.3.1; command introduced.

Related Commands

spb bvlan	Creates a SPB backbone VLAN (BVLAN).
show spb isis bvlans	Displays the SPB BVLAN configuration for the switch.

MIB Objects

```
alcatelIND1IsisSpbEctStaticTable
   alcatelIND1IsisSpbEctStaticEntryBaseVid
   alcatelIND1IsisSpbEctStaticEntryMulticastMode
```

spb isis bridge-priority

Configures the bridge priority value for the SPB bridge. This value is used to rank an SPB bridge in relation to other bridges.

spb isis bridge-priority *priority*

Syntax Definitions

priority	A bridge priority value. The valid range is 0–65535.

Defaults

By default, the bridge priority value for the switch is set to 32768.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The lower the bridge priority number assigned, the higher the priority that is associated with the bridge.
- The bridge priority value makes up the upper two bytes of the eight-byte SPB bridge ID. The lower six bytes of the Bridge ID contain the system ID, which is the dedicated bridge MAC address of the SPB bridge.
- Setting a different bridge priority value on different SPB bridges will override the system identifier significance during the shortest path tree (SPT) calculation.

Examples

```
-> spb isis bridge-priority 15
-> spb isis bridge-priority 32768
```

Release History

Release 7.3.1; command introduced.

Related Commands

show spb isis info	Displays the status and configuration information for the SPB bridge.

MIB Objects

```
alcatelIND1IsisSpbSys
   alcatelIND1IsisSpbSysBridgePriority
```

spb isis interface

Configures the specified port or link aggregate as an ISIS-SPB interface on which protocol data units (PDUs) are sent and received to detect neighbors and form adjacencies with other SPB bridges in the network.

spb isis interface {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} [admin-state {enable | disable} [hello-interval** *seconds***] [hello-multiplier** *count***] [metric** *metric***]**

no spb isis interface [port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Administratively enables the SPB interface.
disable	Administratively disables the SPB interface.
seconds	The amount of time, in seconds, to wait between each transmission of a hello packet from this interface. The valid range is 1–20000.
count	An integer value that is multiplied by the hello interval time to determine the amount of time, in seconds, a receiving bridge holds onto the hello packets transmitted from this interface. The valid range is 2–100.
metric	An integer value that specifies the link cost to reach the destination BMAC. The valid range is 1–16777215.

Defaults

parameter	default
enable | disable	**enable**
seconds	**9**
count	**3**
metric	**10**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the ISIS-SPB interface.
- When configuring a link aggregate as an SPB interface, make sure the link aggregate ID number already exists in the switch configuration.

- All SPB interfaces are automatically assigned to all existing BVLANs. There is one ISIS-SPB instance per switch, and each BVLAN and SPB interface are associated with that instance.
- If the SPB interface metric value is set to a different value for each side of a link, the highest metric value is applied to the entire link.
- Administratively enabling ISIS-SPB on the switch triggers ISIS hello packet transmissions on all SPB interfaces.
- SPB interfaces are typically the Network Network Interface (NNI) ports that carry encapsulated customer data traffic through the Provider Backbone Bridging (PBB) network.
- Note that configuring a port or link aggregate as an SPB interface does not prevent configuration of other VLAN tagging on that port. In other words, the SPB interface can forward regular traffic for other VLAN types in addition to encapsulated SPBM traffic.

Examples

```
-> spb isis interface port 4/7
-> spb isis interface port 4/7 hello-interval 60
-> spb isis interface linkagg 3
-> spb isis interface linkagg 3 hello-multiplier 10
-> spb isis interface port 1/10 hello-interval 20 hello-multiplier 5 metric 2
-> no spb isis interface port 4/7
-> no spb isis interface linkagg 3
```

Release History

Release 7.3.1; command introduced.

Related Commands

show spb isis interface	Displays the ISIS-SPB interface configuration for the bridge.

MIB Objects

```
alcatelIND1IsisSpbAdjStaticTable
   alcatelIND1IsisSpbAdjStaticEntryIfIndex
   alcatelIND1IsisSpbAdjStaticEntryMetric
   alcatelIND1IsisSpbAdjStaticEntryHelloInterval
   alcatelIND1IsisSpbAdjStaticEntryHelloMultiplier
   alcatelIND1IsisSpbAdjStaticEntryIfAdminState
```

spb ipvpn bind

Binds a virtual routing and forwarding (VRF) instance, a Shortest Path Bridging (SPB) service instance identifier (ISID), and an IP gateway together to enable the bidirectional exchange of routes between the VRF and SPB ISID via the Global Route Manager (GRM).

spb ipvpn bind vrf {*vrf_name* **| default} isid** *instance_id* **gateway** *ip_address* **{all-routes | import-route-map** *route_map_name***}**

no spb ipvpn bind vrf {*vrf_name* **| default} isid** *instance_id* **gateway** *ip_address*

Syntax Definitions

vrf_name | **default**	The name of an existing VRF instance for which routes are imported from the Global Routing Table (GRT) to ISIS-SPB. Enter **default** to specify the default VRF instance.
instance_id	An existing ISID that identifies a Shortest Path Bridging (SPB) service in a provider backbone bridge (PBB) network.
ip_address	The IPv4 address of an IP interface that is associated with the specified VRF instance.
all-routes	Imports or exports all routes for this bind entry.
route_map_name	The name of an existing route map to use for filtering VRF routes that are imported from the GRT to ISIS-SPB for this bind entry. There is no filtering from ISIS-SPB to the GRT.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the VRF-ISID bind entry. When the bind is deleted, all routes imported and exported for this binding are retracted.
- The specified VRF name, ISID, gateway IP address, and optional route map name must already exist in the local switch configuration. In addition, the specified route map must exist in the default VRF instance.
- Only one ISID can be bound to a single VRF/gateway IP instance.
- The VRF-ISID binding is only active when the VRF exists, the ISID is configured on the local switch, and the gateway IP address is associated with an active IP interface that is associated with the VRF instance.
- An active "bind" entry causes ISIS-SPB to export learned routes from the SPB network to the GRM and triggers the GRM to send IP routes from the corresponding VRF to ISIS-SPB using the ISID and gateway IP address as the next hop.

- IP routing over SPB requires an L3 VPN interface that serves as an IP gateway to access remote networks. There are two options for defining an L3 VPN interface:
  - Configuring a service-based IP interface for in-line routing (OmniSwitch 9900 only).
  - Configuring an external loopback port configuration in which a pair of loopback ports provide connectivity between VRFs and SPB service access points (SAPs).

Examples

```
-> spb ipvpn bind vrf1 isid 1000 gateway 10.1.1.1 all-routes
-> spb ipvpn bind vrf2 isid 2000 gateway 20.2.2.1 import-route-map rm_vrf2
-> no spb ipvpn bind vrf1 isid 1000 gateway 10.1.1.1
```

Release History

Release 7.3.2; command introduced.

Related Commands

spb ipvpn redist	Configures the redistribution of routes from a VRF to an ISID or from one ISID to another ISID.
show spb ipvpn bind	Displays VRF-to-ISID bindings that enable the import and export of routes between VRFs and ISIDs.

MIB Objects

```
alcatelIND1IsisSpbIPVPNBindTable
   alcatelIND1IsisSpbIPVPNBindVrfName
   alcatelIND1IsisSpbIPVPNBindIsid
   alcatelIND1IsisSpbIPVPNBindGatewayType
   alcatelIND1IsisSpbIPVPNBindGateway
   alcatelIND1IsisSpbIPVPNBindImportRouteMap
   alcatelIND1IsisSpbIPVPNBindRowStatus
```

spb ipvpn redist

Configures the redistribution of routes from a VRF to an ISID or from one ISID to another ISID.

spb ipvpn redist {source-vrf {*vrf_name* **| default} | source-isid** *instance_id***} destination-isid** *instance_id* **{all-routes | route-map** *route_map_name***}**

no spb ipvpn redist {source-vrf *vrf_name* **| source-isid** *instance_id***} destination-isid** *instance_id*

Syntax Definitions

vrf_name | **default**	The source VRF instance from which routes are redistributed. Enter **default** to specify the default VRF instance.
source-isid *instance_id*	The source ISID from which routes are redistributed.
destination-isid *instance_id*	The destination ISID to which routes from either the source VRF or source ISD are redistributed.
all-routes	Imports or exports all routes for this bind entry.
route_map_name	The name of an existing route map to use for filtering routes that are redistributed.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the redistribution entry.
- The specified VRF name, ISID, and optional route map name must already exist in the local switch configuration.
- A redistribution entry is only active when the ISID belongs to an active bind entry. This applies to both ISIDs when redistributing between a source and destination ISID.
- An ISID cannot be bound and redistributed to the same VRF instance.
- The difference between a bind entry and a redistribution entry is as follows:
  - A bind entry binds only one I-SID to one VRF/gateway IP instance. IP VPN routes are then imported and exported bidirectionally between the VRF and I-SID.
  - A redistribution entry allows multiple VRFs to redistribute routes into one I-SID. However, IP VPN routes are only redistributed into the I-SID; there is no bidirectional exchange of routes between the VRF and I-SID. Redistribution is mainly used when routing between I-SIDs is required.

Examples

```
-> spb ipvpn redist source-isid 1000 destination-isid 2000 all-routes
-> spb ipvpn redist source-isid 2000 destination-isid 1000 all-routes
-> spb ipvpn redist source-vrf vrf1 destination-isid 3000 route-map rm_isid2000
```

```
-> no spb ipvpn redist source-vrf vrf1 destination-isid 3000
-> no spb ipvpn redist source-isid 2000 destination isid 1000
```

Release History

Release 7.3.2; command introduced.

Related Commands

spb ipvpn bind	Binds a VRF instance, an ISID, and an IP gateway together to enable the bidirectional exchange of routes between the VRF and ISID via the GRM.
show spb ipvpn redist	Displays the SPB IPVPN redistribution configuration for the switch.

MIB Objects

```
alcatelIND1IsisSpbIPVPNRedistVrfTable
   alcatelIND1IsisSpbIPVPNRedistVrfSourceVrf
   alcatelIND1IsisSpbIPVPNRedistVrfDestIsid
   alcatelIND1IsisSpbIPVPNRedistVrfInetType
   alcatelIND1IsisSpbIPVPNRedistVrfRouteMap
   alcatelIND1IsisSpbIPVPNRedistVrfRowStatus
alcatelIND1IsisSpbIPVPNRedistIsidTable
   alcatelIND1IsisSpbIPVPNRedistIsidSourceIsid
   alcatelIND1IsisSpbIPVPNRedistIsidDestIsid
   alcatelIND1IsisSpbIPVPNRedistVrfInetType
   alcatelIND1IsisSpbIPVPNRedistIsidRouteMap
   alcatelIND1IsisSpbIPVPNRedistIsidRowStatus
```

show spb ipvpn bind

Displays VRF-to-ISID bindings that enable the import and export of routes between VRFs and ISIDs.

show spb ipvpn bind [vrf {*vrf_name* **| default}] [isid** *instance_id***]**

Syntax Definitions

vrf_name | **default**	The name of a VRF instance that is associated with an SPB IPVPN binding. Enter **default** to specify the default VRF instance.
instance_id	An ISID number that is associated with an SPB IPVPN binding.

Defaults

By default, all SPB IPVPN bindings are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **vrf** and **isid** parameters to display the configuration for specific bindings.

Examples

```
-> show spb ipvpn bind
Legend: * indicates bind entry is active
SPB IPVPN Bind Table:
       VRF              ISID            Gateway                 Route-Map
--------------------+------------+---------------------+----------------------
* ospf                  4001         1.1.1.2
* ospf1                 4003         2.2.2.2

Total Bind Entries: 2
```

output definitions

VRF	The name of the VRF instance associated with this binding.
ISID	The ISID number associated with this binding.
Gateway	The gateway IP address associated with this binding. This is the IP address specified for an IP interface that is associated with the VRF in this binding.
Route-Map	The name of an IP route map or **All Routes**.

Release History

Release 7.3.2; command introduced.

Related Commands

spb ipvpn bind	Binds a VRF instance, an ISID, and an IP gateway together to enable the bidirectional exchange of routes between the VRF and ISID via the GRM.
show spb ipvpn redist	Displays the SPB IP VPN redistribution configuration for the switch.
show spb ipvpn route-table	Displays the contents of the SPB IPVPN route table.

MIB Objects

```
alcatelIND1IsisSpbIPVPNBindTable
   alcatelIND1IsisSpbIPVPNBindVrfName
   alcatelIND1IsisSpbIPVPNBindIsid
   alcatelIND1IsisSpbIPVPNBindGatewayType
   alcatelIND1IsisSpbIPVPNBindGateway
   alcatelIND1IsisSpbIPVPNBindRouteMap
```

show spb ipvpn redist

Displays the SPB IPVPN redistribution configuration for the switch. This configuration controls the redistribution of IP VPN routes from ISID to ISID or from VRF to ISID.

show spb ipvpn redist [vrf | [isid]

Syntax Definitions

vrf	Displays the VRF redistribution table.
isid	Displays the ISID redistribution table.

Defaults

By default, both the VRF and ISID redistribution tables are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **isid** parameter to display the contents of the ISID redistribution table (ISID to ISID).
- Use the **vrf** parameter to display the contents of the VRF redistribution table (VRF to ISID).

Examples

```
-> show spb ipvpn redist
Legend: * indicates redist entry is active
SPB IPVPN Redist ISID Table:
  Source-ISID           Destination-ISID     Route-Map
----------------------+--------------------+--------------------
* 4001                 4003
* 4003                 4001

Total Redist ISID Entries: 2

Legend: * indicates redist entry is active
SPB IPVPN Redist VRF Table:
  Source-VRF            Destination-ISID     Route-Map
----------------------+--------------------+--------------------

Total Redist Vrf Entries: 0

-> show spb ipvpn redist isid
Legend: * indicates redist entry is active
SPB IPVPN Redist ISID Table:
  Source-ISID           Destination-ISID     Route-Map
----------------------+--------------------+--------------------
* 4001                 4003
* 4003                 4001

Total Redist ISID Entries: 2
```

```
-> show spb ipvpn redist vrf
Legend: * indicates redist entry is active
SPB IPVPN Redist VRF Table:
  Source-VRF           Destination-ISID     Route-Map
---------------------+--------------------+--------------------

Total Redist Vrf Entries: 0
```

output definitions

Source-ISID	The ISID number from which routes are redistributed to the destination ISID.
Source-VRF	The name of the VRF instance from which routes are redistributed to the destination ISID.
Destination-ISID	The ISID number to which routes are redistributed from another ISID or from a VRF instance.
Route-Map	The name of an IP route map that is used to filter the redistributed routes.

Release History

Release 7.3.2; command introduced.

Related Commands

spb ipvpn redist	Configures the redistribution of routes from a VRF to an ISID or from one ISID to another ISID.
show spb ipvpn bind	Displays the VRF-ISID binding configuration.
show spb ipvpn route-table	Displays the contents of the SPB IPVPN route table.

MIB Objects

```
alcatelIND1IsisSpbIPVPNRedistIsidTable
   alcatelIND1IsisSpbIPVPNRedistIsidSourceIsid
   alcatelIND1IsisSpbIPVPNRedistIsidDestIsid
   alcatelIND1IsisSpbIPVPNRedistRouteMap
alcatelIND1IsisSpbIPVPNRedistVrfTable
   alcatelIND1IsisSpbIPVPNRedistVrfSourceVrf
   alcatelIND1IsisSpbIPVPNRedistVrfDestIsid
   alcatelIND1IsisSpbIPVPNRedistRouteMap
```

show spb ipvpn route-table

Displays the contents of the SPB IPVPN route table.

show spb ipvpn route-table [isid *instance_id***]**

Syntax Definitions

instance_id	An ISID number.

Defaults

By default, all routes for all ISIDs are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **isid** parameter to display information for specific ISID routes.

Examples

```
-> show spb ipvpn route-table
Legend: * indicates IPVPN route has matching locally configured ISID
SPB IPVPN Route Table:
                                                 Source Bridge
     ISID  Destination         Gateway           (Name : BMAC)               Metric
---------+-------------------+-----------------+---------------------------+------
*    4001  1.1.1.0/24           1.1.1.1         L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  1.1.1.0/24           1.1.1.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  2.2.2.0/24           1.1.1.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  10.10.10.0/24        1.1.1.1         L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  15.1.1.0/24          1.1.1.1         L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  15.1.2.0/24          1.1.1.1         L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  15.1.3.0/24          1.1.1.1         L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  15.1.4.0/24          1.1.1.1         L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  15.1.5.0/24          1.1.1.1         L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  20.20.20.0/24        1.1.1.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  25.1.1.0/24          1.1.1.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  25.1.2.0/24          1.1.1.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  25.1.3.0/24          1.1.1.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  25.1.4.0/24          1.1.1.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  25.1.5.0/24          1.1.1.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  1.1.1.0/24           2.2.2.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  2.2.2.0/24           2.2.2.1         L2-DUT2 : 00:e0:b1:dd:99:db     1
*    4003  2.2.2.0/24           2.2.2.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  10.10.10.0/24        2.2.2.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  15.1.1.0/24          2.2.2.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  15.1.2.0/24          2.2.2.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  15.1.3.0/24          2.2.2.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  15.1.4.0/24          2.2.2.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  15.1.5.0/24          2.2.2.2         L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  20.20.20.0/24        2.2.2.1         L2-DUT2 : 00:e0:b1:dd:99:db     1
```

```
*    4003  25.1.1.0/24          2.2.2.1          L2-DUT2 : 00:e0:b1:dd:99:db    1
*    4003  25.1.2.0/24          2.2.2.1          L2-DUT2 : 00:e0:b1:dd:99:db    1
*    4003  25.1.3.0/24          2.2.2.1          L2-DUT2 : 00:e0:b1:dd:99:db    1
*    4003  25.1.4.0/24          2.2.2.1          L2-DUT2 : 00:e0:b1:dd:99:db    1
*    4003  25.1.5.0/24          2.2.2.1          L2-DUT2 : 00:e0:b1:dd:99:db    1

Routes: 30
```

output definitions

ISID	The ISID number associated with this route.
Destination	Destination IP address. Also includes the prefix length notation after the address to indicate the number of bits that are significant in the IPv6 address (mask).
Gateway	IP address of the gateway from which this route was learned.
Source Bridge (Name : BMAC)	The name and BMAC address of the SPB BEB switch that advertised the route.
Metric	The metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.

Release History

Release 7.3.2; command introduced.

Related Commands

show spb ipvpn redist	Displays the SPB IPVPN redistribution configuration for the switch.
show spb ipvpn bind	Displays the VRF-ISID binding configuration.

MIB Objects

```
alcatelIND1IsisSpbIPVPNRouteTable
   alcatelIND1IsisSpbIPVPNRouteIsid
   alcatelIND1IsisSpbIPVPNRoutePrefixType
   alcatelIND1IsisSpbIPVPNRoutePrefix
   alcatelIND1IsisSpbIPVPNRoutePrefixLen
   alcatelIND1IsisSpbIPVPNRouteGateway
   alcatelIND1IsisSpbIPVPNRouteNodeName
   alcatelIND1IsisSpbIPVPNRouteMetric
```

spb ipvpn6 bind

Binds a virtual routing and forwarding (VRF) instance, a Shortest Path Bridging (SPB) service instance identifier (ISID), and an IPv6 gateway together to enable the bidirectional exchange of routes between the VRF and SPB ISID via the Global Route Manager (GRM).

spb ipvpn6 bind vrf {*vrf_name* **| default} isid** *instance_id* **gateway** *ipv6_address* **{all-routes | import-route-map** *route_map_name***}**

no spb ipvpn6 bind vrf {*vrf_name* **| default} isid** *instance_id* **gateway** *ipv6_address*

Syntax Definitions

vrf_name | **default**	The name of an existing VRF instance for which routes are imported from the Global Routing Table (GRT) to ISIS-SPB. Enter **default** to specify the default VRF instance.
instance_id	An existing ISID that identifies a Shortest Path Bridging (SPB) service in a provider backbone bridge (PBB) network.
ipv6_address	The IPv6 address of an IPv6 interface that is associated with the specified VRF instance.
all-routes	Imports or exports all routes for this bind entry.
route_map_name	The name of an existing route map to use for filtering VRF routes that are imported from the GRT to ISIS-SPB for this bind entry. There is no filtering from ISIS-SPB to the GRT.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the VRF-ISID bind entry. When the bind is deleted, all routes imported and exported for this binding are retracted.
- The specified VRF name, ISID, gateway IPv6 address, and optional route map name must already exist in the local switch configuration. In addition, the specified route map must exist in the default VRF instance.
- Only one ISID can be bound to a single VRF/gateway IPv6 instance.
- The VRF-ISID binding is only active when the VRF exists, the ISID is configured on the local switch, and the gateway IPv6 address is associated with an active IPv6 interface that is associated with the VRF instance.
- An active "bind" entry causes ISIS-SPB to export learned routes from the SPB network to the GRM and triggers the GRM to send IPv6 routes from the corresponding VRF to ISIS-SPB using the ISID and gateway IPv6 address as the next hop.

- IPv6 routing over SPB requires an L3 VPN interface that serves as an IPv6 gateway to access remote networks. There are two options for defining an L3 VPN interface:
  - Configuring a service-based IPv6 interface for in-line routing (OmniSwitch 9900 only).
  - Configuring an external loopback port configuration in which a pair of loopback ports provide connectivity between VRFs and SPB service access points (SAPs).

Examples

```
-> spb ipvpn6 bind vrf1 isid 1000 gateway 1000::1 all-routes
-> spb ipvpn6 bind vrf2 isid 2000 gateway 2000::1 import-route-map rm_vrf2
-> no spb ipvpn6 bind vrf1 isid 1000 gateway 1000::1
```

Release History

Release 8.5R2; command introduced.

Related Commands

spb ipvpn6 redist	Configures the redistribution of routes from a VRF to an ISID or from one ISID to another ISID.
show spb ipvpn6 bind	Displays VRF-to-ISID bindings that enable the import and export of routes between VRFs and ISIDs.

MIB Objects

```
alcatelIND1IsisSpbIPVPNBindTable
   alcatelIND1IsisSpbIPVPNBindVrfName
   alcatelIND1IsisSpbIPVPNBindIsid
   alcatelIND1IsisSpbIPVPNBindGatewayType
   alcatelIND1IsisSpbIPVPNBindGateway
   alcatelIND1IsisSpbIPVPNBindImportRouteMap
   alcatelIND1IsisSpbIPVPNBindRowStatus
```

spb ipvpn6 redist

Configures the redistribution of IPv6 routes from a VRF to an ISID or from one ISID to another ISID.

spb ipvpn6 redist {source-vrf {*vrf_name* **| default} | source-isid** *instance_id***} destination-isid** *instance_id* **{all-routes | route-map** *route_map_name***}**

no spb ipvpn6 redist {source-vrf *vrf_name* **| source-isid** *instance_id***} destination-isid** *instance_id*

Syntax Definitions

vrf_name | **default**	The source VRF instance from which routes are redistributed. Enter **default** to specify the default VRF instance.
source-isid *instance_id*	The source ISID from which routes are redistributed.
destination-isid *instance_id*	The destination ISID to which routes from either the source VRF or source ISD are redistributed.
all-routes	Imports or exports all routes for this bind entry.
route_map_name	The name of an existing route map to use for filtering routes that are redistributed.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the redistribution entry.
- The specified VRF name, ISID, and optional route map name must already exist in the local switch configuration.
- A redistribution entry is only active when the ISID belongs to an active bind entry. This applies to both ISIDs when redistributing between a source and destination ISID.
- An ISID cannot be bound and redistributed to the same VRF instance.
- The difference between a bind entry and a redistribution entry is as follows:
  - A bind entry binds only one I-SID to one VRF/ IPv6 gateway instance. IPv6 VPN routes are then imported and exported bidirectionally between the VRF and I-SID.
  - A redistribution entry allows multiple VRFs to redistribute routes into one I-SID. However, IPv6 VPN routes are only redistributed into the I-SID; there is no bidirectional exchange of routes between the VRF and I-SID. Redistribution is mainly used when routing between I-SIDs is required.

Examples

```
-> spb ipvpn6 redist source-isid 1000 destination-isid 2000 all-routes
-> spb ipvpn6 redist source-isid 2000 destination-isid 1000 all-routes
```

```
-> spb ipvpn6 redist source-vrf vrf1 destination-isid 3000 route-map rm_isid2000
-> no spb ipvpn6 redist source-vrf vrf1 destination-isid 3000
-> no spb ipvpn6 redist source-isid 2000 destination isid 1000
```

Release History

Release 8.5R2; command introduced.

Related Commands

spb ipvpn6 bind	Binds a VRF instance, an ISID, and an IPv6 gateway together to enable the bidirectional exchange of routes between the VRF and ISID via the GRM.
show spb ipvpn6 redist	Displays the SPB IPv6 VPN redistribution configuration for the switch.

MIB Objects

```
alcatelIND1IsisSpbIPVPNRedistIsidTable
   alcatelIND1IsisSpbIPVPNRedistIsidSourceIsid
   alcatelIND1IsisSpbIPVPNRedistIsidDestIsid
   alcatelIND1IsisSpbIPVPNRedistIsidInetType
   alcatelIND1IsisSpbIPVPNRedistIsidRouteMap
   alcatelIND1IsisSpbIPVPNRedistIsidRowStatus
alcatelIND1IsisSpbIPVPNRedistVrfTable
   alcatelIND1IsisSpbIPVPNRedistVrfSourceVrf
   alcatelIND1IsisSpbIPVPNRedistVrfDestIsid
   alcatelIND1IsisSpbIPVPNRedistVrfInetType
   alcatelIND1IsisSpbIPVPNRedistVrfRouteMap
   alcatelIND1IsisSpbIPVPNRedistVrfRowStatus
```

show spb ipvpn6 bind

Displays VRF-to-ISID bindings that enable the import and export of IPv6 routes between VRFs and ISIDs.

show spb ipvpn6 bind [vrf {*vrf_name* **| default}] [isid** *instance_id***]**

Syntax Definitions

vrf_name | **default**	The name of a VRF instance that is associated with an SPB IPv6 VPN binding. Enter **default** to specify the default VRF instance.
instance_id	An ISID number that is associated with an SPB IPv6 VPN binding.

Defaults

By default, all SPB IPv6 VPN bindings are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **vrf** and **isid** parameters to display the configuration for specific bindings.

Examples

```
-> show spb ipvpn6 bind
Legend: * indicates bind entry is active
SPB IPVPN Bind Table:
       VRF              ISID            Gateway                 Route-Map
--------------------+------------+----------------------+----------------------
* ospf                   4001         1000::1
* ospf1                  4003         2000::1

Total Bind Entries: 2
```

output definitions

VRF	The name of the VRF instance associated with this binding.
ISID	The ISID number associated with this binding.
Gateway	The gateway IPv6 address associated with this binding. This is the IPv6 address configured for an IPv6 interface that is associated with the VRF in this binding.
Route-Map	The name of an IPv6 route map or **All Routes**.

Release History

Release 8.5R2; command introduced.

Related Commands

spb ipvpn6 bind	Binds a VRF instance, an ISID, and an IPv6 gateway together to enable the bidirectional exchange of routes between the VRF and ISID via the GRM.
show spb ipvpn6 redist	Displays the SPB IPv6 VPN redistribution configuration for the switch.
show spb ipvpn6 route-table	Displays the contents of the SPB IPv6 VPN route table.

MIB Objects

```
alcatelIND1IsisSpbIPVPNBindTable
   alcatelIND1IsisSpbIPVPNBindVrfName
   alcatelIND1IsisSpbIPVPNBindIsid
   alcatelIND1IsisSpbIPVPNBindGatewayType
   alcatelIND1IsisSpbIPVPNBindGateway
   alcatelIND1IsisSpbIPVPNBindRouteMap
```

show spb ipvpn6 redist

Displays the SPB IPv6 VPN redistribution configuration for the switch. This configuration controls the redistribution of IPv6 VPN routes from ISID to ISID or from VRF to ISID.

show spb ipvpn6 redist [vrf | [isid]

Syntax Definitions

vrf	Displays the VRF redistribution table.
isid	Displays the ISID redistribution table.

Defaults

By default, both the VRF and ISID redistribution tables are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **isid** parameter to display the contents of the ISID redistribution table (ISID to ISID).
- Use the **vrf** parameter to display the contents of the VRF redistribution table (VRF to ISID).

Examples

```
-> show spb ipvpnv6 redist
Legend: * indicates redist entry is active
SPB IPVPN Redist ISID Table:
  Source-ISID           Destination-ISID     Route-Map
----------------------+--------------------+--------------------
* 4001                 4003
* 4003                 4001

Total Redist ISID Entries: 2

Legend: * indicates redist entry is active
SPB IPVPN Redist VRF Table:
  Source-VRF            Destination-ISID     Route-Map
----------------------+--------------------+--------------------

Total Redist Vrf Entries: 0

-> show spb ipvpn6 redist isid
Legend: * indicates redist entry is active
SPB IPVPN Redist ISID Table:
  Source-ISID           Destination-ISID     Route-Map
----------------------+--------------------+--------------------
* 4001                 4003
* 4003                 4001

Total Redist ISID Entries: 2
```

```
-> show spb ipvpn6 redist vrf
Legend: * indicates redist entry is active
SPB IPVPN Redist VRF Table:
  Source-VRF           Destination-ISID     Route-Map
---------------------+--------------------+--------------------

Total Redist Vrf Entries: 0
```

output definitions

Source-ISID	The ISID number from which IPv6 routes are redistributed to the destination ISID.
Source-VRF	The name of the VRF instance from which IPv6 routes are redistributed to the destination ISID.
Destination-ISID	The ISID number to which IPv6 routes are redistributed from another ISID or from a VRF instance.
Route-Map	The name of an IPv6 route map that is used to filter the redistributed routes.

Release History

Release 8.5R2; command introduced.

Related Commands

spb ipvpn6 redist	Configures the redistribution of IPv6 routes from a VRF to an ISID or from one ISID to another ISID.
show spb ipvpn6 bind	Displays the VRF-ISID binding configuration.
show spb ipvpn6 route-table	Displays the contents of the SPB IPv6 VPN route table.

MIB Objects

```
alcatelIND1IsisSpbIPVPNRedistIsidTable
   alcatelIND1IsisSpbIPVPNRedistIsidSourceIsid
   alcatelIND1IsisSpbIPVPNRedistIsidDestIsid
   alcatelIND1IsisSpbIPVPNRedistRouteMap
alcatelIND1IsisSpbIPVPNRedistVrfTable
   alcatelIND1IsisSpbIPVPNRedistVrfSourceVrf
   alcatelIND1IsisSpbIPVPNRedistVrfDestIsid
   alcatelIND1IsisSpbIPVPNRedistRouteMap
```

show spb ipvpn6 route-table

Displays the contents of the SPB IPv6 VPN route table.

show spb ipvpn6 route-table [isid *instance_id***]**

Syntax Definitions

instance_id	An ISID number.

Defaults

By default, all IPv6 routes for all ISIDs are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **isid** parameter to display information for specific ISID routes.

Examples

```
-> show spb ipvpn6 route-table
Legend: * indicates IPVPN6 route has matching locally configured ISID
SPB IPVPN6 Route Table:
                                                 Source Bridge
     ISID  Destination         Gateway           (Name : BMAC)               Metric
---------+--------------------+-----------------+---------------------------+------
*    4001  1501:0001::/32       1000::1          L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  1601:0001::/32       1000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  1701:0001::/32       1000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  1901:0001::/32       1000::1          L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  2708:3455::/32       1000::1          L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  2708:3456::/32       1000::1          L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  2708:3457::/32       1000::1          L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  2708:3458::/32       1000::1          L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  2708:3459::/32       1000::1          L2-DUT1 : 00:e0:b1:db:c3:65     1
*    4001  2801:0001::/32       1000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  2901:0001::/32       1000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  2901:0002::/32       1000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  2901:0003::/32       1000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  2901:0004::/32       1000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4001  2901:0005::/32       1000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  1501:0001::/32       2000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  1601:0001::/32       2000::1          L2-DUT2 : 00:e0:b1:dd:99:db     1
*    4003  1701:0001::/32       2000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  1901:0001::/32       2000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  2708:3455::/32       2000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  2708:3456::/32       2000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  2708:3457::/32       2000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  2708:3458::/32       2000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  2708:3459::/32       2000::2          L2-DEV1 : e8:e7:32:00:23:f9     1
*    4003  2801:0001::/32       2000::1          L2-DUT2 : 00:e0:b1:dd:99:db     1
```

```
*    4003  2901:0001::/32       2000::1          L2-DUT2 : 00:e0:b1:dd:99:db    1
*    4003  2901:0002::/32       2000::1          L2-DUT2 : 00:e0:b1:dd:99:db    1
*    4003  2901:0003::/32       2000::1          L2-DUT2 : 00:e0:b1:dd:99:db    1
*    4003  2901:0004::/32       2000::1          L2-DUT2 : 00:e0:b1:dd:99:db    1
*    4003  2901:0005::/32       2000::1          L2-DUT2 : 00:e0:b1:dd:99:db    1

Routes: 30
```

output definitions

ISID	The ISID number associated with this route.
Destination	Destination IPv6 address. Also includes the prefix length notation after the address to indicate the number of bits that are significant in the IPv6 address (mask).
Gateway	IPv6 address of the gateway from which this route was learned.
Source Bridge (Name : BMAC)	The name and BMAC address of the SPB BEB switch that advertised the route.
Metric	The metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.

Release History

Release 8.5R2; command introduced.

Related Commands

show spb ipvpn6 redist	Displays the SPB IPv6 VPN redistribution configuration for the switch.
show spb ipvpn6 bind	Displays the VRF-ISID binding configuration.

MIB Objects

```
alcatelIND1IsisSpbIPVPNRouteTable
   alcatelIND1IsisSpbIPVPNRouteIsid
   alcatelIND1IsisSpbIPVPNRoutePrefixType
   alcatelIND1IsisSpbIPVPNRoutePrefix
   alcatelIND1IsisSpbIPVPNRoutePrefixLen
   alcatelIND1IsisSpbIPVPNRouteGateway
   alcatelIND1IsisSpbIPVPNRouteNodeName
   alcatelIND1IsisSpbIPVPNRouteMetric
```

spb isis admin-state

Enables or disables the administrative status of ISIS-SPB instance for the switch.

spb isis admin-state {enable | disable}

Syntax Definitions

enable	Administratively enables ISIS-SPB for the switch.
disable	Administratively disables ISIS-SPB for the switch.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

When the ISIS-SPB status is disabled, the configuration settings and related statistics of the protocol remain unaffected.

Examples

```
-> spb isis admin-state enable
-> spb isis admin-state disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbSys
   alcatelIND1IsisSpbSysAdminState
```

spb isis area-address

Configures the area address for the ISIS-SPB instance.

spb isis area-address *area_address*

Syntax Definitions

area_address	A 3-byte integer that specifies the ISIS-SPB area address to join.

Defaults

By default, the area address is set to 0.0.0. for ISIS-SPB.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The area address is entered in decimal format with this command but is converted and sent out as a hex value on the wire. For example, if the decimal value entered is “73.00.00”, then the hex value actually sent out on the wire is “49.00.00”.
- The default setting of 0.0.0 is the area address typically used for ISIS-SPB.
- Changing the area address with this command is allowed, but make sure to configure each bridge that will participate in the ISIS-SPB instance with the same area address value.
- ISIS-SPB and ISIS-IP instances may co-exist on the same bridge.

Examples

```
-> spb isis area-address 1.1.1
-> spb isis area-address 0.0.0
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbSys
   alcatelIND1IsisSpbSysAreaAddress
```

spb isis source-id

Configures the shortest path (SP) source identifier value for the SPB bridge. This value identifies the source of multicast frames and is relevant only in multicast tandem replication mode.

spb isis source- id {*source_id* **| auto}**

Syntax Definitions

source_id	A source identifier entered as *xx-xx-xx*, where *xx* is a hexadecimal value.
auto	Changes the source ID back to the default value.

Defaults

By default, the last three least significant bytes of the system ID is used for the source ID.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The source ID is the high order 3 bytes for the Group Address DA for the SPB bridge. Note that only 20 bits are used; the top 4 bits are not used.

Examples

```
-> spb isis source-id 00-2a-1d
-> spb isis source-id 07-0b-d3
-> spb isis source-id auto
```

Release History

Release 7.3.1; command introduced.

Related Commands

show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbSys
   alcatelIND1IsisSpbmSysSPSourceId
```

spb isis control-address

Changes the ISIS-SPB control MAC address, which is used as the destination address for ISIS-SPB control packets.

spb isis control-address {alll1 | alll2 | allis}

Syntax Definitions

alll1	All Level 1 Intermediate Systems **(**01:80:C2:00:00:14).
alll2	All Level 2 Intermediate Systems (01:80:C2:00:00:15).
allis	All Intermediate Systems (09:00:2B:00:00:05).

Defaults

By default, the control MAC address is set to AllL1.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Changing the ISIS-SPB control MAC address on the OmniSwitch can enhance interoperability with third-party ISIS-SPB devices.

Examples

```
-> spb isis control-address alll1
-> spb isis control-address alll2
-> spb isis control-address allis
```

Release History

Release 7.3.2; command introduced.

Related Commands

show spb isis info	Displays the status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbSys
   alcatelIND1IsisSpbSysControlAddr
```

spb isis spf-wait

Configures the time intervals between the first, second, and subsequent ISIS-SPB shortest path first (SPF) calculations.

spb isis spf-wait [initial-wait *milliseconds* **| second-wait** *milliseconds***| max-wait** *milliseconds***]**

Syntax Definitions

initial-wait *milliseconds*	Specifies the number of milliseconds to wait before triggering an initial SPF calculation after a topology change. The valid range is 10–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.
second-wait *milliseconds*	Specifies the minimum number of milliseconds to wait between the first and second SPF calculation. The valid range is 1–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.
max-wait *milliseconds*	Specifies the maximum number of milliseconds to wait between two consecutive SPF calculations. Enter a value that is the same or greater than the second wait time value. The valid range is 1000–120000 milliseconds.

Defaults

parameter	default
max-wait *milliseconds*	1000
initial-wait *milliseconds*	100
second-wait *milliseconds*	300

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- To reset all three of the SPF wait time intervals back to their default values, use the **spb isis spf-wait** command without specifying any parameters.
- Subsequent SPF calculations, if required, are generated at exponentially increasing intervals of the SPF **second-wait** parameter value until the **maximum-wait** parameter value is reached. For example, if the second-wait interval value is set to 1000 milliseconds, then the next SPF calculation is triggered after 2000 milliseconds and the next SPF calculation after that is triggered at 4000 milliseconds, and so on, until the maximum-wait interval value is reached.
- When the maximum interval value is reached, the SPF wait interval will stay at the maximum value until there are no more SPF calculations scheduled during that interval. After a full interval without any SPF calculations, the SPF wait interval will reset back to the **initial-wait** parameter interval value.

Examples

```
-> spb isis spf-wait max-wait 2500 initial-wait 1000 second-wait 1500
-> spb isis spf-wait max-wait 5000
-> spb isis spf-wait initial-wait 1000
-> spb isis spf-wait second-wait 2000
-> spb isis spf-wait
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis lsp-wait	Configures the time intervals between the first, second, and subsequent generation of link state PDUs (LSPs).
show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbProtocolConfig
   alcatelIND1IsisSpbProtocolSpfMaxWait
   alcatelIND1IsisSpbProtocolSpfInitialWait
   alcatelIND1IsisSpbProtocolSpfSecondWait
```

spb isis lsp-wait

Configures the time intervals between the first, second and subsequently generated link state PDU (LSP).

spb isis lsp-wait {max-wait *milliseconds* **| initial-wait** *milliseconds* **| second-wait** *milliseconds***}**

Syntax Definitions

max-wait *milliseconds*	Specifies the maximum number of seconds to wait between two consecutively generated LSPs. Enter a value that is the same or greater than the second wait time value. The valid range is 1000–120000 milliseconds.
initial-wait *milliseconds*	Specifies the number of seconds to wait before triggering an initial LSP generation after a topology change. The valid range is 0–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.
second-wait *milliseconds*	Specifies the minimum number of seconds to wait between the first and second generated LSPs. The valid range is 1000–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.

Defaults

parameter	default
max-wait *milliseconds*	1000
initial-wait *milliseconds*	0
second-wait *milliseconds*	300

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- To reset all three of the LSP wait time intervals back to their default values, use the **spb isis lsp-wait** command without specifying any parameters.
- Subsequent LSP, if required, are generated at exponentially increasing intervals of the LSP **second-wait** parameter value until the **maximum-wait** parameter value is reached. For example, if the second-wait interval value is set to 10 seconds, then the next LSP is generation is triggered after 20 seconds and the next LSP generated after that is triggered at 40 seconds, and so on, until the maximum-wait interval value is reached.
- When the maximum interval value is reached, the LSP wait interval will stay at the maximum value until there are no more LSP generations during that interval. After a full interval without any LSP generations, the LSP wait interval will reset back to the **initial-wait** parameter interval value.

Examples

```
-> spb isis lsp-wait max-wait 2000 initial-wait 1000 second-wait 1500
-> spb isis lsp-wait max-wait 5000
-> spb isis lsp-wait initial-wait 2500
-> spb isis lsp-wait second-wait 3000
-> spb isis lsp-wait
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis spf-wait	Configures the time intervals between the first, second, and subsequent shortest path first (SPF) calculations.
show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbProtocolConfig
   alcatelIND1IsisSpbProtocolLspMaxWait
   alcatelIND1IsisSpbProtocolLspInitialWait
   alcatelIND1IsisSpbProtocolLspSecondWait
```

spb isis rapid-lsp-converge

Configures the status of ISIS-SPB rapid link state PDU (LSP) convergence and reserves an SPB I-SID to identify a multicast domain. When rapid LSP convergence is enabled (the default) and a topology event occurs, LSP frames are flooded on the multicast domain to all participating SPB bridges to expedite network notification and convergence time.

spb isis rapid-lsp-converge {isid *instance_id* **| admin-state {enable | disable}}**

Syntax Definitions

instance_id	An SPB service instance identifier (I-SID). The valid range is 256–16777214 (or 0.1.0–255.255.254 in dot-decimal notation format).
enable	Enables rapid LSP convergence.
disable	Disables rapid LSP convergence.

Defaults

By default, rapid LSP convergence is enabled for the switch and the I-SID number is set to 16776961 or 255.255.1.

Platforms Supported

OmniSwitch 9900

Usage Guidelines

- The reserved I-SID is always associated with the control BVLAN and is only modifiable when rapid LSP convergence is disabled.
- When changing the default I-SID value, make sure the new value specified is not associated with any SPB service. The specified I-SID will be reserved only for rapid LSP convergence.

Examples

```
-> spb isis rapid-lsp-convergence admin-state disable
-> spb isis rapid-lsp-convergence isid 4001
-> spb isis rapid-lsp-convergence isid 220.1.1
-> spb isis rapid-lsp-convergence admin-state enable
```

Release History

Release 8.5R2; command was introduced.

Related Commands

show spb isis rapid-lsp-converge-info	Displays the ISIS-SPB rapid LSP convergence information for the switch.
show spb isis rapid-lsp-converge-table	Displays the multicast forwarding information for all of the SPB bridges that are participating in rapid LSP convergence.

MIB Objects

```
alcatelIND1ISISSpbRapidLspConvergence
   alcatelIND1ISISSpbRapidLspConvergenceAdminStatus
   alcatelIND1ISISSpbRapidLspConvergenceIsid
```

spb isis overload

Configures the LSP database overload state for the local ISIS-SPB switch and optionally specifies the amount of time the switch remains in this state. When the overload state is enabled, the switch signals to other ISIS-SPB switches that it is not able to accept transit traffic.

spb isis overload [timeout *seconds***]**

no spb isis overload

Syntax Definitions

seconds	Specifies the timeout interval, in seconds. The valid range is 60–1800.

Defaults

By default, the IS-IS overload state is disabled.

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to make the router exit the overload state.
- If the time period is not specified, the router remains in the overload state for an infinite period.
- During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is used only if the destination route is directly reachable by the router (for example, it will not be used for other transit traffic).
- This command can be used when the router is overloaded or before executing a shutdown command to divert traffic around the router.

Examples

```
-> spb isis overload timeout 70
-> no spb isis overload
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis overload-on-boot	Configures the ISIS-SPB instance to operate in an overload state during bootup for a specified time period.
show spb isis info	Displays status and configuration information for the ISIS-SPB instance.

MIB Objects

```
alcatelIND1IsisSpbSysSetOverload
alcatelIND1IsisSpbSysOverloadTimeout
alcatelIND1IsisSpbSysOverloadStatus
```

spb isis overload-on-boot

Configures the ISIS-SPB switch to operate in the overload state after a system bootup for the specified amount of time.

spb isis overload-on-boot [timeout *seconds***]**

no spb isis overload-on-boot

Syntax Definitions

seconds	Specifies the timeout interval, in seconds. The valid range is 60–1800.

Defaults

By default, the ISIS-SPB switch will not operate in the overload state after a bootup.

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to prevent the switch from entering the overload state after bootup.
- This command configures the switch to operate in the overload state after a bootup and until the timeout value expires or the **no** form of this command is used.
- The **no spb isis overload** command does not influence the overload-on-boot function.

Examples

```
-> spb isis overload-on-boot timeout 80
-> no spb isis overload-on-boot
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis overload	Sets the ISIS-SPB switch to operate in the overload state.
show spb isis info	Displays status and configuration information for the ISIS- SPB instance.

MIB Objects

```
vRtrIsisTable
   alcatelIND1IsisSpbSysOverloadOnBoot
   alcatelIND1IsisSpbSysOverloadOnBootTimeout
   alcatelIND1IsisSpbSysOverloadStatus
```

spb isis graceful-restart

Configures graceful restart of the bridge. It allows ISIS-SPB to reconverge faster, minimizing service interruption.

spb isis graceful-restart

no spb isis graceful-restart

Syntax Definitions

N/A

Defaults

By default, the graceful restart functionality is enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable graceful restart and remove the graceful restart configuration from the SPB bridge.
- When graceful restart is enabled, the bridge can either be a helper (which helps a neighbor router to restart) or a restarting router, or both.

Examples

```
-> spb isis graceful-restart
-> no spb isis graceful-restart
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis graceful-restart helper	Configures the helper mode of routers for graceful restart.
show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbProtocolConfig
   alcatelIND1IsisSpbProtocolGracefulRestart
```

spb isis graceful-restart helper

Administratively enables and disables the ISIS-SPB bridge to operate in the helper mode in response to a bridge performing a graceful restart.

spb isis graceful-restart helper {enable | disable}

Syntax Definitions

enable	Enables the helper mode on the bridge.
disable	Disables the helper mode on the bridge.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

When graceful restart is enabled, the helper mode is enabled by default.

Examples

```
-> spb isis graceful-restart helper disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis graceful-restart	Configures graceful restart on the bridge.
show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbProtocolConfig
   alcatelIND1IsisSpbProtocolGRHelperMode
```

show spb isis info

Displays the global ISIS-SPB status and configuration information for the SPB bridge.

show spb isis info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show spb isis info
SPB ISIS Bridge Info:
  System Id             = e8e7.3233.1831,
  System Hostname       = BEB-1,
  SPSourceID            = 03-18-31,
  SPBM System Mode      = auto,
  BridgePriority        = 32768 (0x8000),
  MT ID                 = 0,
  Control BVLAN         = 4001,
  Area Address          = 0.0.0,
  Level Capability      = L1,
  Admin State           = UP,
  LSDB Overload         = Disabled,
  Last Enabled          = Thu Aug  2 22:43:19 2012,
  Last SPF              = Fri Aug  3 18:15:51 2012,
  SPF Wait              = Max: 1000 ms, Initial: 100 ms, Second: 300 ms,
  LSP Lifetime          = 1200,
  LSP Wait              = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
  Graceful Restart      = Disabled,
  GR helper-mode        = Disabled,
  # of L1 LSPs          = 8
  Control Address       = 01:80:c2:00:00:14 (AllL1)
```

output definitions

System Id	The system ID of the SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
System Hostname	The system name assigned to the SPB bridge. Configured through the **system name** command.

output definitions (continued)

SPSourceID	The shortest path (SP) source ID value for the SPB bridge. This value identifies the source of multicast frames and is relevant only in the multicast tandem replication mode. Configured through the **spb isis source-id** command.
SPBM System Mode	Indicates if the SP source ID was manually set (**manual**) using the **spb isis source-id** command or automatically allocated (**auto**) using the last three least significant bytes of the System ID.
BridgePriority	The bridge priority value assigned to the SPB bridge. Configured through the **spb isis bridge-priority** command.
MT ID	The IS-IS Multi Topology ID.
Control BVLAN	The SPB base VLAN assigned to exchange ISIS-SPB control traffic with other SPB bridges. Configured through the **spb isis control-bvlan** command.
Area Address	The IS-IS area address for this ISIS-SPB instance. Configured through the **spb isis area-address** command.
Level Capability	The level capability of the bridge. Only Level 1 **(L1**) is supported.
Admin State	The state of the SPB instance for the bridge (**Up** or **Down**). Configured through the **spb isis admin-state** command.
LSDB Overload	The LSP database overload state of the switch. Configured through the **spb isis overload** command.
Last Enabled	The date and time when the ISIS-SPB instance was last enabled for the bridge.
Last SPF	The date and duration of the last shortest path first (SPF) calculation.
SPF Wait	The SPF wait time intervals used to trigger SPF calculations after a topology change. Configured through the **spb isis spf-wait** command.
LSP Lifetime	The Lifetime of the LSP, in seconds.
LSP Wait	The LSP wait time intervals used to trigger LSP generations. Configured through the **spb isis lsp-wait** command.
Graceful Restart	Indicates if graceful restart is **Enabled** or **Disabled**. Configured through the **spb isis graceful-restart** command.
GR helper-mode	Indicates if the graceful restart helper mode is **Enabled** or **Disabled**. Configured through the **spb isis graceful-restart helper** command.
# of L1 LSPs	The number of LSPs for Level-1 adjacency.
Control Address	The destination MAC address used for ISIS-SPB control frames. Configured through the **spb isis control-address** command.

Release History

Release 7.3.1; command was introduced.
Release 7.3.2; **Control Address** field added.

Related Commands

show spb isis spf	Displays the shortest path first (SPF) information to all known SPB bridges for a specific BVLAN.
show spb isis bvlans	Displays the ISIS-SPB backbone VLAN (BVLAN) configuration for the bridge.
show spb isis interface	Displays the ISIS-SPB network interface configuration for the bridge.

MIB Objects

```
alcatelIND1IsisSpbSys
   alcatelIND1IsisSpbSysId
   alcatelIND1IsisSpbSysName
   alcatelIND1IsisSpbmSysSPSourceId
   alcatelIND1IsisSpbmSysMode
   alcatelIND1IsisSpbSysBridgePriority
   alcatelIND1IsisSpbSysControlBvlan
   alcatelIND1IsisSpbSysAreaAddress
   alcatelIND1IsisSpbSysAdminState
   alcatelIND1IsisSpbProtocolSpfMaxWait
   alcatelIND1IsisSpbProtocolSpfInitialWait
   alcatelIND1IsisSpbProtocolSpfSecondWait
   alcatelIND1IsisSpbProtocolLspMaxWait
   alcatelIND1IsisSpbProtocolLspInitialWait
   alcatelIND1IsisSpbProtocolLspSecondWait
   alcatelIND1IsisSpbProtocolGracefulRestart
   alcatelIND1IsisSpbProtocolGRHelperMode
   alcatelIND1IsisSpbSysControlAddr
```

show spb isis bvlans

Displays the ISIS-SPB backbone VLAN (BVLAN) configuration for the bridge.

show spb isis nodes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command also displays the equal cost tree (ECT) algorithm that is assigned to each BVLAN.

Examples

```
-> show spb isis bvlans
SPB ISIS BVLANS:
                              Services Num    Tandem     Root Bridge
BVLAN   ECT-algorithm In Use  mapped   ISIDS  Multicast  (Name : MAC Address)
------+-------------+-------+--------+-----+----------+--------------------
   501  00-80-c2-01   NO      NO          0  GMODE      BRIDGE-3:00:d1:95:00:30:02
   502  00-80-c2-02   NO      NO          0  SGMODE
   503  00-80-c2-03   YES     NO          4  SGMODE
   504  00-80-c2-04   YES     NO          4  SGMODE

BVLANs:     4
```

output definitions

BVLAN	The VLAN ID number for the SPB BVLAN. Configured through the **spb bvlan** command.
ECT-algorithm	The equal cost tree (ECT) algorithm index (**1–16**) assigned to the BVLAN. Configured through the **spb isis bvlan ect-id** command.
In Use	Indicates whether or not the BVLAN is in use.
Services Mapped	Indicates whether or not any local services are mapped to the BVLAN.
Num ISIDS	The number of services known to the BVLAN.
Tandem Multicast	The tandem multicast mode (**SGMODE** or **GMODE**) for the BVLAN. Configured through the **spb isis bvlan tandem-multicast-mode** command.
Root Bridge (Name : MAC Address)	The system name and bridge MAC address of the root bridge. This value is displayed only for GMODE configurations.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis info	Displays status and configuration information for the SPB instance
show spb isis interface	Displays the ISIS-SPB network interface configuration for the bridge.

MIB Objects

N/A

show spb isis interface

Displays the ISIS-SPB network interface configuration for the switch.

show spb isis interface

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command also shows the operational and administrative status of the interface.
- When an SPB interface is created, the interface is automatically assigned to each SPB BVLAN in the switch configuration.

Examples

```
-> show spb isis interface
SPB ISIS Interfaces:
                                  Oper   Admin   Link      Hello   Hello
 Interface       Level   CircID   state  state   Metric    Intvl   Mult
---------------+-------+----------+------+-------+---------+-------+-------
 1/1             L1      1        DOWN   UP      10        9       3
 1/2             L1      2        UP     UP      10        9       3
 1/3             L1      3        DOWN   UP      10        9       3
 1/4             L1      4        DOWN   UP      10        9       3
 1/5             L1      5        DOWN   UP      10        9       3
 1/6             L1      6        DOWN   UP      10        9       3
 1/7             L1      7        DOWN   UP      10        9       3
 1/10            L1      9        DOWN   UP      10        9       3

Interfaces : 8
```

output definitions

Interface	The slot/port or link aggregate ID of the SPB interface.
Level	The IS-IS Area Level (L1) for the interface.
CircID	The circuit ID of the interface.
Oper-state	The operational state of the interface (**UP** or **DOWN**).
Admin-state	The administrative state of the interface (**UP** or **DOWN**).
Link Metric	The metric value of the router for the corresponding area level.

output definitions

Hello Interval	The number of seconds the interface waits between Hello PDU transmissions.
Hello Multiplier	The number that is multiplied by the Hello Interval to determine the hold time.

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis interface	Creates an ISIS-SPB network interface.

MIB Objects

```
alcatelIND1IsisSpbAdjStaticTable
   alcatelIND1IsisSpbAdjStaticEntryIfIndex
   alcatelIND1IsisSpbAdjStaticEntryMetric
   alcatelIND1IsisSpbAdjStaticEntryHelloInterval
   alcatelIND1IsisSpbAdjStaticEntryHelloMultiplier
   alcatelIND1IsisSpbAdjStaticEntryIfAdminState
```

show spb isis adjacency

Displays information about the ISIS-SPB adjacencies created for the SPB bridge.

show ip isis adjacency [detail]

Syntax Definitions

detail	Displays additional information about the ISIS-SPB adjacencies.

Defaults

By default, a summary list of adjacency information is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip isis adjacency
SPB ISIS Adjacency:
 System
 (Name : SystemId)                    Type State  Hold  Interface
-------------------------------------+----+------+-----+---------
         bridge2 :  00d0.9506.4c62     L1    UP    27       1/1
         bridge3 :  00d0.9507.9732     L1    UP    20       1/2

Adjacencies : 2
```

output definitions

Name	The system name assigned to the adjacent SPB bridge.
SystemId	The system ID of the adjacent SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
Type	The level (**LI**) of the adjacent bridge.
State	The state of the adjacency (**UP** or **DOWN**).
Hold	The adjacency hold time, in seconds.
Interface	The slot/port or link aggregate ID of the SPB interface on which the adjacency was formed.
Adjacencies	The total number of adjacent SPB bridges.

```
-> show ip isis adjacency detail
SPB ISIS Adjacency detail:
    SystemID: 00d0.9506.4c62 :
      B-MAC        : 00:d0:95:06:4c:62     , Hostname   : bridge2             ,
      Interface    : 1/1                   , Up Time    : Mon Sep 26 17:54:29 2011,
      State        : UP                    , Priority   : 0                  ,
      Hold Time    : 18                    , Max Hold   : 27                 ,
      Adj Level    : L1                    , NLPIDs     : SPB                ,
      ExtLocalCktId(YES): 2,
      Restart Support    : Disabled           ,
      Restart Status     : Not currently being helped,
      Restart Supressed  : Disabled

    SystemID: 00d0.9507.9732 :
      B-MAC        : 00:d0:95:07:97:32     , Hostname   : bridge3             ,
      Interface    : 1/2                   , Up Time    : Mon Sep 26 17:54:29 2011,
      State        : UP                    , Priority   : 0                  ,
      Hold Time    : 21                    , Max Hold   : 27                 ,
      Adj Level    : L1                    , NLPIDs     : SPB                ,
      ExtLocalCktId(YES): 2,
      Restart Support    : Disabled           ,
      Restart Status     : Not currently being helped,
      Restart Supressed  : Disabled

Adjacencies : 1
```

output definitions

SystemID	The system ID of the adjacent SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
B-MAC	The backbone MAC address (system ID) of the adjacent bridge. This is the address that is used as the source address for encapsulated customer traffic that is tunneled through SPB services.
Interface	The slot/port or link aggregate ID of the SPB interface on which the adjacency was formed.
State	The state of the adjacency (**UP** or **DOWN**).
Hold Time	The adjacency hold time, in seconds.
Adj Level	The adjacency level (**L1**) of the SPB bridge.
ExtLocalCktId(YES)	The circuit ID that the peer bridge has assigned to this adjacency.
Restart Support	Indicates if graceful restart is **Enabled** or **Disabled**.
Restart Status	Indicates whether the adjacent SPB bridge is helping the local bridge to restart (**Not currently being helped** or **Currently being helped**).
Restart Suppressed	Indicates whether or not the advertisement of LSPs is suppressed per the request of adjacent SPB bridge (**Enabled** or **Disabled**).
Hostname	The system name assigned to the adjacent SPB bridge.
Up Time	Indicates the time period in seconds, during which the SPB bridge was in the adjacency.
Priority	The bridge priority value of the adjacent SPB bridge.

output definitions

Max Hold	Indicates the maximum hold time of the adjacent SPB bridge.
NLPIDs	The Network Layer Protocol ID (NLPID) of the adjacent bridge (SPB NLPID = 0xC1).

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis database	Displays ISIS-SPB topology information maintained in the link state database (LSDB).
show spb isis nodes	Displays the discovered node-level parameter values for all of the ISIS-SPB bridges participating in the topology.

MIB Objects

N/A

show spb isis database

Displays ISIS-SPB topology information maintained in the link state database (LSDB).

show ip isis database [lsp-id *lsp_id***}]**

Syntax Definitions

lsp_id	The LSP ID.

Defaults

By default, the entire LSDB is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the *lsp-id* parameter with this command to view database information for a specific link state packet (LSP).

Examples

```
-> show spb isis database
      Legends : P    = The Partition repair bit is set
                OV   = The overload bit is set
                ATT  = The Attach bit is set
                L1   = Specifies a Level 1 IS type
                L2   = Specifies a Level 2 IS type
      SPB ISIS LSP Database:
       LSP ID                 Sequence    Checksum   Lifetime   Attributes
      ----------------------+-----------+----------+----------+------------
       00d1.9500.3002.00-00  0x000000a8     0x9bdc        862   L1
       00e0.b188.99be.00-00  0x0000009c     0xa719        762   L1
       e8e7.329a.4b0b.00-00  0x2f6          0x5799        708   L1
      Level-1 LSP count : 3
```

output definitions

LSP ID	The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.
Sequence	The sequence number of the LSP. The sequence number is a value used to identify old and duplicate LSPs.
Checksum	The checksum value of the LSP.
Lifetime	The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the LSDB of all the SPB bridges.
Attributes	The level capability of the bridge. This implementation of ISIS-SPB only supports Level 1 (L1).
LSP Count	The number of LSPs in the LSDB.

```
-> show spb isis database lsp-id e8e7.329a.4b0b.00-00
Legends : P    = The Partition repair bit is set
          OV   = The overload bit is set
          ATT  = The Attach bit is set
          L1   = Specifies a Level 1 IS type
          L2   = Specifies a Level 2 IS type
SPB ISIS LSP Database:
--------------------------------------------------------------------------------
LSP ID        : e8e7.329a.4b0b.00-00                  Level     : L1
Sequence      : 0x2f6           Checksum  : 0x5799    Lifetime  : 708
Version       : 1               Pkt Type  : 18        Pkt Ver   : 1
Attributes    : L1              Max Area  : 3
SysID Len     : 6               Used Len  : 1398      Alloc Len : 1492

TLVs :
Area Addresses      :
   Area Address     : (01) 00
   Area Address     : (03) 00.00.00
Supp Protocols      :
   Protocols        : SPB
IS-Hostname         :
   Hostname         : 0S6860
TE IS Neighbors     :
   Neighbor         : e8e7.329a.57df  SPB Metric 10 Num of Ports 1 Port-Id 0x4(1/4)
MT Capability       :
   MT-ID : 0x0
   SPB INSTANCE     :
     CIST Root-ID: 0x0 0x0
     CIST Ext Root Path Cost: 0x00000000  Bridge Priority: 0x8000
     SPSourceID: 0x001a4b0b (Auto)        Number of Trees: 16
     [#1 ]ECT-algo:0x0080c201 baseVid:4000 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
     [#2 ]ECT-algo:0x0080c202 baseVid:4001 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
     [#3 ]ECT-algo:0x0080c203 baseVid:4002 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
     [#4 ]ECT-algo:0x0080c204 baseVid:4003 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#5 ]ECT-algo:0x0080c205 baseVid:4004 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#6 ]ECT-algo:0x0080c206 baseVid:4005 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#7 ]ECT-algo:0x0080c207 baseVid:4006 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#8 ]ECT-algo:0x0080c208 baseVid:4007 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#9 ]ECT-algo:0x0080c209 baseVid:4008 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#10]ECT-algo:0x0080c20a baseVid:4009 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#11]ECT-algo:0x0080c20b baseVid:4010 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#12]ECT-algo:0x0080c20c baseVid:4011 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#13]ECT-algo:0x0080c20d baseVid:4012 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#14]ECT-algo:0x0080c20e baseVid:4013 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#15]ECT-algo:0x0080c20f baseVid:4014 spVid:0 usedByISID:0()      mode:1(SPBM)
     [#16]ECT-algo:0x0080c210 baseVid:4015 spVid:0 usedByISID:0()      mode:1(SPBM)
MT Capability       :
   MT-ID : 0x0
   SPB SVCID-UCAST-ADDR :
       B-MAC e8.e7.32.9a.4b.0b Base-VID 4000
       [ISID# 1] 16776961 (T=1/R=1)
       [ISID# 2] 1000 (T=0/R=0)
   SPB SVCID-UCAST-ADDR :
       B-MAC e8.e7.32.9a.4b.0b Base-VID 4001
       [ISID# 1] 2000 (T=0/R=0)
   SPB SVCID-UCAST-ADDR :
       B-MAC e8.e7.32.9a.4b.0b Base-VID 4002
       [ISID# 1] 3000 (T=0/R=0)
IP VPN              :
```

```
   MT-ID : 0x0     BVID: 4000   ISID: 1000 (T=0/R=0)
   GATEWAY:
           1.1.1.34
   PREFIX:
           1.1.1.1/32, metric 1
           12.1.1.0/24, metric 1
           13.1.1.0/24, metric 1
           128.251.40.0/24, metric 1
           172.28.4.0/24, metric 1
           34.1.1.0/24, metric 1
IP VPN              :
   MT-ID : 0x0     BVID: 4001   ISID: 2000 (T=0/R=0)
   GATEWAY6:
           1035:1::1
   PREFIX6:
           3021:1:0:26::/64, metric 1
           3021:1:0:27::/64, metric 1
           3021:1:0:28::/64, metric 1
IP VPN              :
   MT-ID : 0x0     BVID: 4002   ISID: 3000 (T=0/R=0)
   GATEWAY6:
           1036:1::1
   PREFIX6:
           3001:1:0:4d::/64, metric 1
IP VPN              :
   MT-ID : 0x0     BVID: 4000   ISID: 1000 (T=0/R=0)
   GATEWAY6:
           1034:1::1
   PREFIX6:
           3001:1:0:4d::/64, metric 1
IP VPN              :
   MT-ID : 0x0     BVID: 4002   ISID: 3000 (T=0/R=0)
   GATEWAY6:
           1036:1::1
   PREFIX6:
           3001:1:0:4c::/64, metric 1
```

Release History

Release 7.3.1; command was introduced.
Release 8.5R2; display output updated to include SPB IPv6 VPN information.

Related Commands

show spb isis adjacency	Displays information about the ISIS-SPB adjacencies created for the SPB bridge.
show spb isis nodes	Displays the discovered node-level parameter values for all of the ISIS-SPB bridges participating in the topology.

MIB Objects

```
N/A
```

show spb isis nodes

Displays the discovered node-level parameter values for all of the ISIS-SPB switches participating in the topology.

show spb isis nodes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the system name, system ID, SPsource ID, and bridge priority parameter values for the bridges discovered within the ISIS-SPB topology.

Examples

```
-> show spb isis nodes
SPB ISIS Nodes:
 System Name          System Id      SourceID BridgePriority
--------------------+--------------+--------+---------------
 Bridge-1             00e0.b1e7.0188  0x70188  32768 (0x8000)
 Bridge-2             00e0.b1e7.0bd3  0x70bd3  32768 (0x8000)
 Bridge-4             e8e7.3200.2a1d  0x02a1d  32768 (0x8000)
 Bridge-5             e8e7.3233.1891  0x31891  32768 (0x8000)
 Bridge-6             e8e7.3233.199d  0x3199d  32768 (0x8000)
 Bridge-7             e8e7.3233.1a29  0x31a29  32768 (0x8000)
 Bridge-8             e8e7.3233.1c81  0x31c81  32768 (0x8000)
```

output definitions

System Name	The system name assigned to the SPB bridge.
System Id	The system ID of the SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
SourceID	The shortest path (SP) source ID value for the SPB bridge. This value identifies the source of multicast frames and is relevant only in the multicast tandem replication mode.
BridgePriority	The bridge priority value assigned to the SPB bridge.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis adjacency	Displays information about the ISIS-SPB adjacencies created for the SPB bridge.
show spb isis info	Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis unicast-table

Displays the unicast forwarding information for the specified BVLANs. Use this command to verify unicast addresses were learned correctly on each SPB switch in the ISIS-SPB backbone topology.

show spb isis unicast-table [bvlan *bvlan_id***]**

Syntax Definitions

bvlan_id	The VLAND ID of an existing BVLAN.

Defaults

By default, the forwarding information for all BVLANs in the SPB topology is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **bvlan** *bvlan_id* parameter to display information for a specific BVLAN.

Examples

```
-> show spb isis unicast-table
SPB ISIS Unicast MAC Table:
        Destination                                Outbound
 BVLAN  (Name : MAC Address)                       Interface
------+-----------------------------------------+-----------
  4001  BRIDGE-2            : 00:e0:b1:e7:0b:d3        1/1
  4001  BRIDGE-4            : e8:e7:32:00:2a:1d        1/1
  4001  BRIDGE-5            : e8:e7:32:33:18:91        1/3
  4001  BRIDGE-6            : e8:e7:32:33:19:9d        1/1
  4001  BRIDGE-7            : e8:e7:32:33:1a:29        1/2
  4001  BRIDGE-8            : e8:e7:32:33:1c:81        1/1
  4002  BRIDGE-2            : 00:e0:b1:e7:0b:d3        1/1
  4002  BRIDGE-4            : e8:e7:32:00:2a:1d        1/3
  4002  BRIDGE-5            : e8:e7:32:33:18:91        1/3
  4002  BRIDGE-6            : e8:e7:32:33:19:9d        1/2
  4002  BRIDGE-7            : e8:e7:32:33:1a:29        1/2
  4002  BRIDGE-8            : e8:e7:32:33:1c:81        1/3
  4003  BRIDGE-2            : 00:e0:b1:e7:0b:d3        1/1
  4003  BRIDGE-4            : e8:e7:32:00:2a:1d        1/3
  4003  BRIDGE-5            : e8:e7:32:33:18:91        1/3
  4003  BRIDGE-6            : e8:e7:32:33:19:9d        1/3
  4003  BRIDGE-7            : e8:e7:32:33:1a:29        1/2
  4003  BRIDGE-8            : e8:e7:32:33:1c:81        1/3
  4004  BRIDGE-2            : 00:e0:b1:e7:0b:d3        1/1
  4004  BRIDGE-4            : e8:e7:32:00:2a:1d        1/1
  4004  BRIDGE-5            : e8:e7:32:33:18:91        1/3
  4004  BRIDGE-6            : e8:e7:32:33:19:9d        1/1
  4004  BRIDGE-7            : e8:e7:32:33:1a:29        1/2
  4004  BRIDGE-8            : e8:e7:32:33:1c:81        1/1
```

```
MAC Addresses: 24
-> show spb isis unicast-table bvlan 4001
SPB ISIS Unicast MAC Table:
        Destination                                Outbound
 BVLAN  (Name : MAC Address)                       Interface
------+-----------------------------------------+-----------
  4001  BRIDGE-2            : 00:e0:b1:e7:0b:d3        1/1
  4001  BRIDGE-4            : e8:e7:32:00:2a:1d        1/1
  4001  BRIDGE-5            : e8:e7:32:33:18:91        1/3
  4001  BRIDGE-6            : e8:e7:32:33:19:9d        1/1
  4001  BRIDGE-7            : e8:e7:32:33:1a:29        1/2
  4001  BRIDGE-8            : e8:e7:32:33:1c:81        1/1

MAC Addresses: 6
```

output definitions

BVLAN	The VLAN ID number for the SPB BVLAN.
System (Name : BMAC)	The system name of the destination SPB bridge, and the destination unicast BMAC address for that bridge.
Outbound Interface	The interface (port or link aggregate) on which the destination system is reached.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis bvlans	Displays status and configuration information for the SPB instance.
show spb isis multicast-table	Displays the multicast forwarding information for the specified service instance identifier (I-SID).

MIB Objects

N/A

show spb isis services

Displays the service instance identifier (I-SID) mapping for bridges participating in the SPB topology. This command provides a network-wide view of existing services to help verify that SPB services are correctly advertised and learned by ISIS-SPB.

show spb isis services [isid *instance_id* **| bvlan** *bvlan_id***]**

Syntax Definitions

instance_id	An existing I-SID number.
bvlan_id	The VLAND ID of an existing BVLAN.

Defaults

By default, the mapping for all I-SIDs in the SPB topology is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **isid** *instance_id* number to display information for a specific service instance.
- Use the **bvlan** *bvlan_id* parameter to display information for a specific BVLAN.

Examples

```
-> show spb isis services
Legend: * indicates locally configured ISID
SPB ISIS Services Info:
                      System
    ISID      BVLAN   (Name : BMAC)                              MCAST(T/R)
------------+-------+-----------------------------------------+-----------
*     1000     4001   BRIDGE-1            : 00:e0:b1:e7:01:88
*     1000     4001   BRIDGE-4            : e8:e7:32:00:2a:1d
*     1001     4001   BRIDGE-1            : 00:e0:b1:e7:01:88
*     1001     4001   BRIDGE-4            : e8:e7:32:00:2a:1d
*     1002     4001   BRIDGE-1            : 00:e0:b1:e7:01:88
*     1002     4001   BRIDGE-4            : e8:e7:32:00:2a:1d
*     1003     4001   BRIDGE-1            : 00:e0:b1:e7:01:88
*     1003     4001   BRIDGE-4            : e8:e7:32:00:2a:1d
*     1004     4001   BRIDGE-1            : 00:e0:b1:e7:01:88
*     1004     4001   BRIDGE-4            : e8:e7:32:00:2a:1d
*     1005     4001   BRIDGE-1            : 00:e0:b1:e7:01:88
*     1005     4001   BRIDGE-4            : e8:e7:32:00:2a:1d
*     1006     4001   BRIDGE-1            : 00:e0:b1:e7:01:88
*     1006     4001   BRIDGE-4            : e8:e7:32:00:2a:1d
*     1007     4001   BRIDGE-1            : 00:e0:b1:e7:01:88
*     1007     4001   BRIDGE-4            : e8:e7:32:00:2a:1d

ISIDs:    16
```

output definitions

ISID	The service instance identifier.
BVLAN	The VLAN ID number for the SPB BVLAN.
System (Name : BMAC)	The system name of the SPB bridge from where the I-SID was discovered or configured, and the destination unicast BMAC address to which frames associated with the service instance are sent.
Multicast (T/R)	Indicates the multicast service requirement for the instance (**T**ransmit, **R**eceive, or **both**).

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis info	Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis spf

Displays the shortest path first (SPF) information to all known SPB bridges for a specific BVLAN.

show spb isis spf bvlan *bvlan_id* **[bmac** *mac_address***]**

Syntax Definitions

bvlan_id	The VLAND ID of an existing BVLAN.
mac_address	An SPB bridge BMAC address.

Defaults

By default, the SPF information for all known BMAC addresses for the specified BVLAN.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **bmac** *mac_address* parameter to display information for a specific SPB bridge.

Examples

```
-> show spb isis spf bvlan 4001
SPB ISIS Path Table:
Destination                   Outbound  Next Hop                      SPB     Num
(Name : BMAC)                 Interface (Name : BMAC)                 Metric  Hops
-----------------------------+---------+-----------------------------+------+------
BRIDGE-1  : 00:e0:b1:e7:01:88    1/3    BRIDGE-2  : 00:e0:b1:e7:0b:d3   20    2
BRIDGE-2  : 00:e0:b1:e7:0b:d3    1/3    BRIDGE-2  : 00:e0:b1:e7:0b:d3   10    1
BRIDGE-4  : e8:e7:32:00:2a:1d    1/2    BRIDGE-4  : e8:e7:32:00:2a:1d   10    1
BRIDGE-5  : e8:e7:32:33:18:91    1/1    BRIDGE-5  : e8:e7:32:33:18:91   10    1
BRIDGE-6  : e8:e7:32:33:19:9d    1/3    BRIDGE-2  : 00:e0:b1:e7:0b:d3   20    2
BRIDGE-7  : e8:e7:32:33:1a:29    1/3    BRIDGE-2  : 00:e0:b1:e7:0b:d3   30    3

SPF Path count: 6

-> show spb isis spf bvlan 4001 bmac e8:e7:32:33:1a:29
SPB ISIS Path Details:
 Path Hop Name        Path Hop BMAC
--------------------+------------------
 BRIDGE-7            e8:e7:32:33:1a:29
 BRIDGE-1            00:e0:b1:e7:01:88
 BRIDGE-2            00:e0:b1:e7:0b:d3
```

output definitions

Destination (Name : BMAC)	The system name of the destination SPB bridge, and the destination BMAC address for that bridge.
Outbound Interface	The interface (port or link aggregate) on which the destination system is reached.

output definitions (continued)

Next Hop (Name : BMAC)	The system name of the next-hop SPB bridge, and the BMAC address for that bridge.
SPB Metric	The metric (cost) to reach the destination BMAC address.
Num Hops	The number of hops along the path to the destination.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis multicast-sources-spf	Displays the SPF reachability for a known multicast source bridge for a specific BVLAN.
show spb isis info	Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis multicast-table

Displays the multicast forwarding information for the specified service instance identifier (I-SID).

show spb isis multicast-table [isid *instance_id***]**

Syntax Definitions

instance_id	An existing I-SID number.

Defaults

By default, the forwarding information for all services in the SPB topology is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **isid** *instance_id* parameter to display information for a specific service instance.

Examples

```
-> show spb isis multicast-table
SPB ISIS Multicast MAC Table:
                                  MCAST Source                  Inbound   Outbound
 ISID  BVLAN MCAST Group Address  (Name:BMAC)                  Interface Interface
------+-----+------------------+-----------------------------+---------+---------
 2000    41   0a:fd:c2:00:01:22   BRIDGE-8  : 00:d0:95:0a:fd:c2   1/2       1/3

 MAC Addresses: 1
```

output definitions

ISID	The service instance identifier.
BVLAN	The VLAN ID number for the SPB BVLAN associated with the service instance.
MCAST Group Address	The multicast destination group address.
MCAST Source (Name : BMAC)	The system name and BMAC address of the multicast source.
Inbound Interface	The interface (port or link aggregate) on which multicast traffic is received for the service instance.
Outbound Interface	The interface (port or link aggregate) on which multicast traffic is sent for the service instance.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis multicast-sources	Displays all the known multicast sources across the SPB domain and BVLANs.
show spb isis multicast-sources-spf	Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.

MIB Objects

N/A

show spb isis multicast-sources

Displays all the known multicast sources across the SPB domain and BVLANs.

show spb isis multicast-sources

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command also displays whether or not the source is reachable.

Examples

```
-> show spb isis multicast-sources
SPB ISIS Multicast Source Nodes:
 Multicast Source
 (Name : BMAC)                  Reachable   (# ) BVIDS
------------------------------+---------+-----------------
 BRIDGE-8  : 00:d0:95:0a:fd:c2    YES      (#2) 4001 4002

 Total SPB Multicast Source Nodes: 1
```

output definitions

Multicast Source (Name : BMAC)	The system name and BMAC address of the multicast source bridge.
Reachable	Indicates whether the multicast source node is reachable (**YES** or **NO**).
(#) BVIDS	Indicates the number of BVLANs and the BVLAN IDs on which the bridge acts as a multicast source.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis multicast-sources-spf	Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.
show spb isis multicast-table	Displays the multicast forwarding information for the specified service instance identifier (I-SID).
show spb isis info	Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis multicast-sources-spf

Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.

show spb isis multicast-sources-spf bvlan *bvlan_id* **bmac** *mac_address* **[dest** *mac_address***]**

Syntax Definitions

bvlan_id	The VLAN ID of an existing BVLAN.
mac_address	An SPB bridge BMAC address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **dest** *mac_address* parameter to display information for a specific SPB bridge.

Examples

```
-> show spb isis multicast-sources-spf bvlan 4001 bmac 00:d0:95:0a:fd:c2
SPB ISIS Path Table:
Destination                   Outbound  Next Hop                    SPB     Num
(Name : BMAC)                 Interface (Name : BMAC)               Metric  Hops
----------------------------+---------+---------------------------+------+------
BRIDGE-1 : 00:d0:95:03:19:12     1/1   BRIDGE-7 : 00:d0:95:09:79:02   30     3
BRIDGE-2 : 00:d0:95:06:4c:62     1/1   BRIDGE-7 : 00:d0:95:09:79:02   20     2
BRIDGE-3 : 00:d0:95:07:97:32     1/1   BRIDGE-7 : 00:d0:95:09:79:02   20     2
BRIDGE-6 : 00:d0:95:08:f2:12     1/2   BRIDGE-6 : 00:d0:95:08:f2:12   10     1
BRIDGE-7 : 00:d0:95:09:79:02     1/1   BRIDGE-7 : 00:d0:95:09:79:02   10     1

SPF Path count: 5

-> show spb isis spf bvlan 4001 bmac 00:d0:95:0a:fd:c2 dest 00:d0:95:03:19:12
SPB ISIS Multicast Source Path Details:
 Path Hop Name        Path Hop BMAC
--------------------+------------------
 BRIDGE-1            00:d0:95:03:19:12
 BRIDGE-3            00:d0:95:07:97:32
 BRIDGE-7            00:d0:95:09:79:02
```

output definitions

Destination (Name : BMAC)	The system name and BMAC address of the destination SPB bridge.
Outbound Interface	The interface (port or link aggregate) on which the destination system is reached.

output definitions (continued)

Next Hop (Name : BMAC)	The system name and BMAC address of the next-hop SPB bridge.
SPB Metric	The metric (cost) to reach the destination BMAC address.
Num Hops	The number of hops along the path to the destination.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis multicast-sources	Displays all the known multicast sources across the SPB domain and BVLANs.
show spb isis multicast-table	Displays the multicast forwarding information for the specified service instance identifier (I-SID).
show spb isis spf	Displays the SPF information to all known SPB bridges for a specific BVLAN.
show spb isis info	Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis ingress-mac-filter

Displays the ingress MAC filter for multicast traffic for a given BVLAN operating in the (*,G) mode.

show spb isis ingress-mac-filter [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*] | bvlan *bvlan_id* **| bmac** *mac_address*]

Syntax Definitions

chassis	The chassis identifier.
slot/port[-*port2*]	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id[-*agg_id2*]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
bvlan_id	The VLAND ID of an existing BVLAN.
mac_address	The source MAC address of the multicast traffic allowed on the specified BVLAN and physical port.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the optional command parameters to display specific information with this command.
- Each of the optional command parameters can be combined with any of the other optional parameters within the same command line.

Examples

```
-> show spb isis ingress-mac-filter
SPB ISIS Ingress MAC Table (for GMODE bvlans only):
        Inbound     Multicast source MAC
 BVLAN  Interface   (Name : MAC Address)
------+-----------+---------------------------------------
   40        1/1    BRIDGE-1            : 00:d0:95:04:8d:92

MAC Addresses: 1
```

output definitions

BVLAN	The VLAN ID number for the SPB BVLAN.
Inbound Interface	The interface (port or link aggregate) on which the multicast source MAC was received.
System (Name : BMAC)	The system name and MAC address of the multicast traffic source.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis info	Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis rapid-lsp-converge-info

Displays the status of ISIS-SPB rapid LSP convergence for the SPB bridge.

show spb isis rapid-lsp-converge-info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9900

Usage Guidelines

N/A

Examples

```
-> show spb isis rapid-lsp-converge-info
SPB ISIS Rapid Lsp Converge Info:
  Status                = DOWN,
  Control ISID          = 255.255.1(0xffff01)
```

output definitions

Status	The status of the ISIS-SPB rapid LSP convergence for the bridge (**Up** or **Down**).
Control ISID	The SPB I-SID number that is reserved for rapid LSP convergence.

Release History

Release 8.5R2; command was introduced.

Related Commands

spb isis rapid-lsp-converge	Configures the status of ISIS-SPB rapid LSP convergence.
show spb isis rapid-lsp-converge-table	Displays the multicast forwarding information for all of the SPB bridges that are participating in rapid LSP convergence.

MIB Objects

```
alcatelIND1IsisSpbRapidLspConvergence
   alcatelIND1IsisSpbRapidLspConvergenceAdminState
   alcatelIND1IsisSpbRapidLspConvergenceIsid
```

show spb isis rapid-lsp-converge-table

Displays the multicast forwarding information for all the SPB bridges that are participating in rapid LSP convergence.

show spb isis rapid-lsp-converge-table

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 9900

Usage Guidelines

N/A

Examples

```
-> show spb isis rapid-lsp-converge-table
SPB ISIS Multicast MAC Table:
                                        MCAST Source                Inbound   Outbound
 ISID     BVLAN MCAST Group Address (Name:BMAC)                      Interface Interface
---------+-----+------------------+--------------------------+---------+---------
255.255.1 4000  43:d2:72:ff:ff:01   BEB_29_2 :e8:e7:32:e4:d2:72  1/6/14
255.255.1 4000  53:08:04:ff:ff:01   BEB_25_8 :e8:e7:32:8c:36:0d  1/6/14
255.255.1 4000  d3:d9:00:ff:ff:01   BEB_25_7 :e8:e7:32:7d:d9:00  1/6/14

MAC Addresses: 3
```

output definitions

ISID	The service instance identifier.
BVLAN	The VLAN ID number for the SPB BVLAN associated with the service instance.
MCAST Group Address	The multicast destination group address.
MCAST Source (Name : BMAC)	The system name and BMAC address of the multicast source.
Inbound Interface	The interface (port or link aggregate) on which multicast traffic is received for the service instance.
Outbound Interface	The interface (port or link aggregate) on which multicast traffic is sent for the service instance.

Release History

Release 8.5R2; command was introduced.

Related Commands

spb isis rapid-lsp-converge	Configures the status of ISIS-SPB rapid LSP convergence.
show spb isis rapid-lsp-converge-info	Displays the status of ISIS-SPB rapid LSP convergence for the SPB bridge.

MIB Objects

N/A

10 Service Manager Commands

The OmniSwitch supports the following service types:

- Shortest Path Bridging MAC (SPBM), as defined in the IEEE 802.1aq standard. The SPBM network topology consists of two layers: the backbone infrastructure (control plane) layer and the services (data plane) layer. ISIS-SPB builds the backbone layer by defining loop-free paths through the backbone network. The service layer is based on the PBB framework as defined in the IEEE 802.1ah standard. SPBM supports the MAC-in-MAC method for data encapsulation. An SPBM service transports the encapsulated traffic over the ISIS-SPB infrastructure.
- Virtual eXtensible LAN (VXLAN), as defined in the IETF "VXLAN: A Framework for Overlaying Layer 2 Virtualized Networks over Layer 3 Networks" standard. VXLAN is a Layer 2 overlay network that is used to segment and tunnel device traffic. The backbone (control plane) layer is built through a flooding and learning process. A VXLAN service transports encapsulated traffic through the network. This allows Layer 2 communication between local and remote devices over a Layer 3 network.
- Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel. Similar to the OmniSwitch VXLAN implementation, L2 GRE provides a Layer 2 overlay network that is used to isolate and tunnel device traffic between tunnel end points over the underlying IP network.
  - L2 GRE assumes that the tunnel end points (IP addresses) are reachable for tunneling traffic; configuring static routes or routing protocols (such as RIP or OSPF) to ensure end point reachability is required. The BFD protocol can be used to learn the ARP of the next-hop gateway.
  - On switches that will operate as a tunnel aggregation switch, L2 GRE services and associated service objects are configured through Service Manager commands to create multiple tunnel end points.
  - On switches that will operate as a tunnel access switch, a single tunnel end point is created by configuring a UNP profile that defines L2 GRE service parameters. When qualifying traffic is assigned to the profile, the necessary L2 GRE service objects are dynamically created. See Chapter 39, "Access Guardian Commands," for information about how to configure an L2 GRE UNP profile.

The OmniSwitch Service Manager application provides the ability to configure and manage a service-based architecture consisting of the following logical entities that are required to provision a service:

- **Access Port**—A port or link aggregate configured as a service access port. This type of port defines the point at which traffic from other provider networks or traffic directly from customer networks enters the network infrastructure. The access port is also associated with a Layer 2 profile that specifies how to process protocol control frames received on the port.
- **SPBM, VXLAN, or L2 GRE Service—**A flooding domain for network traffic. A service defines a Virtual Forwarding Instance (VFI) that is capable of learning device MAC addresses from the access side and from the network side and then switching the traffic based on this information.
- **Service Access Point (SAP)—**A SAP is a logical service entity (also referred to as a virtual port) that binds an access port to an SPB service ID, a VXLAN service ID, or an L2 GRE service ID and

specifies the type of customer traffic (untagged, single-tagged, double-tagged, or all) to encapsulate and tunnel through the network infrastructure.

- **Service Distribution Point (SDP)**—An SDP provides a logical point at which customer traffic is directed from one backbone edge switch to another. SDPs are used to set up distributed services, which consist of at least one SAP on a local node, one SAP on a remote node, and an SDP binding the service on both nodes.
- **Bind-SDP**—Represents the binding of a service instance to an SDP. The SDP then distributes the service connectivity to other backbone edge switches.
- **Service Instance Identifier (I-SID)**—An SPB backbone service instance that will tunnel the encapsulated data traffic through the network infrastructure. The I-SID is bound to an SPB backbone VLAN (BVLAN) ID and a Service Manager SPB service ID when the service is created.
- **Virtual Network Identifier (VNID)**—The VNID is a 24-bit segment ID (also referred to as a VXLAN segment ID) that is used to identify encapsulated VM frames. A VNID is bound to a Service Manager VXLAN service ID when the service is created.
- **Virtual Private Network ID (VPNID)**—An L2 GRE tunnel ID that identifies a segment of a ~~guest~~ tunnel service and is used in the GRE encapsulation header. A VPNID is bound to a Service Manager L2 GRE service ID when the service is created.

This chapter documents the Command Line Interface (CLI) commands used to configure and verify the service-based architecture. For commands used to configure and verify the ISIS-SPB backbone, see Chapter 9, “Shortest Path Bridging Commands.”

MIB information for the Service Manager commands is as follows:

Filename: ALCATEL-IND1-SERVICE-MGR-MIB.mib
Module: alcatelIND1ServiceMgrMIB

A summary of the available commands is listed here:

Service Commands	**service spb** **service vxlan** **service l2gre** **service description** **service multicast-mode** **service stats** **service vlan-xlation** **service admin-state** **service remove-ingress-tag** **service vxlan udp-port** **service vxlan vrf** **service local-vrrp** **service l2gre reserved-vlan** **show service** **show service ports** **show service spb sap** **show service debug-info** **show service info**
Service Access Port Commands	**service l2profile** **service l2profile inbound 802.1ab** **service access** **service access l2profile** **service access vlan-xlation** **show service l2profile** **show service access**

Service Access Point (SAP) Commands	**service sap** **service sap description** **service sap trusted** **service sap stats** **service sap admin-state**
Service Distribution Point (SDP) Commands	**service sdp vxlan** **service sdp l2gre** **service bind-sdp** **service l2gre auto-discover** **show service sdp** **show service sdp spb** **show service sdp vxlan** **show service sdp l2gre** **show service bind-sdp** **show service bind-sdp spb** **show service bind-sdp vxlan** **show service bind-sdp l2gre**
Statistics Commands	**clear service counters** **show service counters**
Remote Fault Propagation (RFP)	**service rfp local-endpoint** **service rfp remote-endpoint** **show service rfp** **show service rfp configuration**

service spb

Configures a Shortest Path Bridging (SPB) service and associates that service with a backbone service instance identifier (I-SID) and BVLAN. An SPB service connects multiple customer sites together across a provider-managed core network by creating a virtual zero-hop, Layer 2 switched domain.

This section describes the base command along with the other optional command keywords that are used to configure SPB service parameter values. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default value.

service *service_id***[-***service_id2***] spb isid** *instance_id***[-***instance_id2***] bvlan** *bvlan_id***[***:x***]**
[description *desc_info***]**
[multicast-mode {head-end | tandem | hybrid}]
[stats {enable | disable}]
[vlan-xlation {enable | disable}]
[admin-state {enable | disable}]

no service *service_id* **spb**

Syntax Definitions

*service_id***[-***service_id2***]**	A unique numerical value to identify a specific SPB service. The valid service ID range is 1–32767. Use a hyphen to configure a range of SPB service IDs (10-13).
*instance_id***[-***instance_id2***]**	A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network. The valid range is 256–16777214. Use a hyphen to configure a range of I-SIDs (300-303).
*bvlan_id***[***:x***]**	The VLAN ID number of an existing SPB BVLAN. To specify a range of BVLANs to assign to a range of services, append the "*:x*" syntax, where "*x*" is the number of BVLANs to assign in sequence (for example, 4000:4 would assign BVLANs 4000, 4001, 4002, and 4003).

Defaults

When an SPB service is created without specifying any of the optional parameter values, the service is created with the following default values:

parameter	default
tandem | head-end | hybrid	**head-end**
description *desc_info*	no description added
stats {enable | disable}	**disable**
vlan-xlation {enable | disable}	**disable**
admin-state {enable | disable}	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- To remove an SPB service, administratively disable the service (including any associated SAPs and SDPs) then use the **no** form of this command and specify the service ID of the disabled service.
- SPB services created with this command are considered static services, which are identified by a service ID number between 1 and 32767 (the valid range for this command). If the SPB service was dynamically created by another OmniSwitch feature, such as Universal Network Profiles (UNP), a service ID number between 32768 and 65534 is automatically assigned to the dynamic service.
- An SPB service provides E-LAN connectivity for customer traffic and is identified by an I-SID. Services are bound to service access ports (SAPs) on the access side. On the network side they are automatically bound to service distribution points by the ISIS-SPB protocol.
- Each SPB service is basically a Virtual Forwarding Instance (VFI) that is capable of learning customer MAC addresses from the access side (SAPs) and from the network side (Mesh SDP) and then switching the traffic based on this information.

Examples

```
-> service 100 spb isid 1000 bvlan 4001
-> service 200 spb isid 2000 bvlan 4001 vlan-xlation enable multicast-mode head-end
description "SPB service for ISID 2000 in Head-end mode"
-> service 1-100 spb isid 1000-1100 bvlan 4000:4 multicast-mode tandem description
"100 SPB Services with ISIDs from 1000-1100 and BVLANs from 4000-4003"
-> no service 100 spb
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for specifying a range of IDs, ISIDs, and BVLANs added.

Related Commands

service description	Modifies the description information for the service.
service multicast-mode	Modifies the multicast replication mode for the service.
service stats	Modifies the status of statistics collection for the service.
service vlan-xlation	Modifies the status of VLAN translation for the service.
service admin-state	Modifies the administrative status for the service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcType
   alaSvcIsid
   alaSvcBVlan
   alaSvcDescription
   alaSvcStatsAdminStatus
   alaSvcMulticastMode
   alaSvcAdminStatus
   alaSvcSapVlanXlation
```

service vxlan

Configures a Virtual eXtensible LAN (VXLAN) service. This section describes the base command along with the other optional command keywords that are used to configure VXLAN service parameter values. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default value.

service *service_id***[-***service_id2***] vxlan vnid {***vxlan_id***[-***vxlan_id2***] |** *xxx.xxx.xxx***[-***xxx.xxx.xxx***]}**
[description *desc_info***]**
[multicast-mode [tandem | head-end | hybrid]
[stats {enable | disable}]
[vlan-xlation {enable | disable}]
[admin-state {enable | disable}]
[remove-ingress-tag {enable | disable}]

no service *service_id* **vxlan**

Syntax Definitions

*service_id***[-***service_id2***]**	A unique numerical value to identify a specific VXLAN service. The valid service ID range is 1–32767. Use a hyphen to specify a range of VXLAN services.
*vxlan_id***[-***vxlan_id2***]**	A 24-bit numerical value that identifies a VXLAN segment (a VXLAN network ID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format). Use a hyphen to specify a range of IDs (25001-25005).

Defaults

When a VXLAN service is created without specifying any of the optional parameter values, the service is created with the following default values:

parameter	default
description *desc_info*	no description added
tandem | head-end | hybrid	**hybrid**
stats {enable | disable}	**disable**
vlan-xlation {enable | disable}	**disable**
admin-state {enable | disable}	**disable**

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32

Usage Guidelines

- To remove a VXLAN service, administratively disable the service then use the **no** form of this command and specify the service ID of the disabled service.

- Configuring a VXLAN service on an OmniSwitch 6900-V72 or OmniSwitch 6900-C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported.
- VXLAN services created with this command are considered static services, which are identified by a service ID number between 1 and 32767 (the valid range for this command). If the VXLAN service was dynamically created by another OmniSwitch feature, such as Universal Network Profiles (UNP), a service ID number between 32768 and 65534 is automatically assigned to the dynamic service.
- A VXLAN service provides E-LAN connectivity for customer traffic and is bound to a Service Access Ports (SAP) on the access side. On the network side, the service is bound to a unicast or multicast Service Distribution Point (SDP).
- Each VXLAN service is basically a Virtual Forwarding Instance (VFI) that is capable of learning customer MAC addresses from the access side (SAPs) and from the network side (mesh SDP) and then switching the traffic based on this information.

Examples

```
-> service 10 vxlan vnid 1000 description "VxLAN service for VNID 1000 in hybrid
multicast mode" admin-state enable
-> service 20 vxlan vnid 2000 multicast-mode head-end description "VxLAN Service
for VNID 2000 in headend mode only" admin-state enable
-> service 30 vxlan vnid 3.173.104 multicast-mode tandem description "VxLAN Service
for VNID 3000 in tandem mode only" admin-state enable
-> service 1-100 vxlan vnid 1000-1100 stats enable description "100 VxLAN Services
with VNIDs from 1000-1100"
-> no service 20 vxlan
```

Release History

Release 7.3.4; command was introduced.

Related Commands

service description	Modifies the description information for the service.
service multicast-mode	Modifies the multicast replication mode for the service.
service stats	Modifies the status of statistics collection for the service.
service vlan-xlation	Modifies the status of VLAN translation for the service.
service admin-state	Modifies the administrative status for the service.
service remove-ingress-tag	Configures whether or not the customer VLAN tag is removed from ingress packets for the specified service.
service vxlan udp-port	Configures the UDP destination port for all encapsulated VXLAN frames.
service vxlan vrf	Configures the current VRF instance for the VXLAN segment.
service sdp vxlan	Manually configures a unicast or multicast VXLAN SDP.
service bind-sdp	Binds VXLAN services to VXLAN SDPs.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcType
   alaSvcVnid
   alaSvcDescription
   alaSvcAdminStatus
   alaSvcAllocationType
   alaSvcStatsAdminStatus
   alaSvcMulticastMode
   alaSvcSapVlanXlation
```

service l2gre

Configures a Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel service. This type of service is used to define an L2 GRE tunnel endpoint. The service is created and bound to a SAP on an OmniSwitch that will serve as a tunnel aggregation switch.

This section describes the base command along with the other optional command keywords that are used to configure L2 GRE tunnel service parameter values. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default value.

service *service_id* **l2gre vpnid {***vpn_id***}**
[description *desc_info***]**
[stats {enable | disable}]
[vlan-xlation {enable | disable}]
[admin-state {enable | disable}]
[remove-ingress-tag {enable | disable}]

no service *service_id* **l2gre**

Syntax Definitions

service_id	A unique numerical value to identify a specific L2 GRE tunnel service. The valid service ID range is 1–32767. Use a hyphen to specify a range of services.
vpn_id	A GRE tunnel Virtual Private Network (VPN) ID. This value should match the VPN ID value used to create the GRE tunnel endpoint on the Guest Tunneling access switch.

Defaults

When an L2 GRE tunnel service is created without specifying any of the optional parameter values, the service is created with the following default values:

parameter	default
description *desc_info*	no description added
stats {enable | disable}	**disable**
vlan-xlation {enable | disable}	**disable**
admin-state {enable | disable}	**enable**
remove-ingress-tag {enable | disable}	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- To remove an L2 GRE tunnel service, administratively disable the service then use the **no** form of this command and specify the service ID of the disabled service.
- L2 GRE tunnel services created with this command are considered static services, which are identified by a service ID number between 1 and 32767 (the valid range for this command). If the L2 GRE service was dynamically created by another OmniSwitch feature, such as Universal Network Profiles (UNP), a service ID number between 32768 and 65534 is automatically assigned to the dynamic service.
- An L2 GRE tunnel service provides connectivity for customer traffic and is bound to a SAP on the access side. On the network side, the service is bound to a unicast Service Distribution Point (SDP).
- Each L2 GRE tunnel service is basically a Virtual Forwarding Instance (VFI) that is capable of encapsulating customer MAC addresses from the access side (SAPs) and from the network side (mesh SDP) and then tunneling the traffic through the network.
- L2 GRE tunneling services do not support multicast modes. All Broadcast, Unknown Unicast, and Multicast (BUM) traffic is replicated; a copy is sent to each far-end node over unicast SDPs (similar to the head-end multicast mode).
- On switches that will operate as a tunnel aggregation switch, L2 GRE services and associated service objects are configured through the **service l2gre**, **service sap**, **service sdp l2gre**, and **service bind-sdp** commands.
- On switches that will operate as a tunnel access switch, the L2 GRE service objects are dynamically created based on the specified configuration for a UNP L2 GRE service profile when qualifying device traffic is assigned to that profile. Refer to Chapter 39, “Access Guardian Commands,” in this guide for information about how to configure a UNP L2 GRE service profile.

Examples

```
-> service 10 l2gre vpnid 1000 description "L2GRE service for VPNID 1000” admin-
state disable
-> service 20 l2gre vpnid 2000 description "L2GRE service for VPNID 2000" vlan-
xlation enable admin-state enable
-> service 30 l2gre vpnid 3000 description "L2GRE service for VPNID 3000” remove-
ingress-tag enable admin-state enable
-> service 40 l2gre vpnid 4000 description "L2GRE service with VPNID 4000" stats
enable admin-state enable
-> service 40 l2gre vpnid 4000 admin-state disable
-> no service 40
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

service description	Modifies the description information for the service.
service stats	Modifies the status of statistics collection for the service.
service vlan-xlation	Modifies the status of VLAN translation for the service.
service admin-state	Modifies the administrative status for the service.
service remove-ingress-tag	Configures whether or not the customer VLAN tag is removed from ingress packets for the specified service.
service sdp l2gre	Manually configures an L2 GRE SDP.
service bind-sdp	Binds L2 GRE services to L2 GRE SDPs.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcType
   alaSvcVpnId
   alaSvcDescription
   alaSvcAdminStatus
   alaSvcAllocationType
   alaSvcStatsAdminStatus
   alaSvcSapVlanXlation
```

service description

Configures a description for the specified service.

service {*service_id* **| all} description** *desc_info*

no service {*service_id* **| all} description**

Syntax Definitions

service_id	An existing service ID number.
all	Applies this command to all service ID numbers.
desc_info	An ASCII text string up to 160 characters in length.

Defaults

By default, a description is not added when the service is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the description from the specified service ID.
- This command adds or modifies a description for an existing service. However, the **description** parameter is also used to specify a description at the time the service is created.

Examples

Adding or modifying a description for an existing service:

```
-> service 100 description "SPB service for ISID 1234"
-> service 200 description “VXLAN service for VNID 24000”
-> service 300 description “L2GRE service for VPNID 30”
-> no service 200 description
```

Configuring a new service with a description:

```
-> service 100 isid 1234 bvlan 3000 description "SPB service for ISID 1234"
-> service 200 vxlan vnid 24000 description “VXLAN service for VNID 24000”
-> service 300 l2gre vpnid 30 description “L2GRE service for VPNID 30”
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service spb	Configures an SPB service.
service vxlan	Configures a VXLAN service.
service multicast-mode	Configures the multicast replication mode for the specified service.
service stats	Configures the statistics collection status for the specified service.
service vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.
service admin-state	Configures the administrative status of the specified service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcDescription
```

service multicast-mode

Configures the multicast replication mode for the specified service.

service {*service_id* **| all} multicast-mode {head-end | tandem | hybrid}**

Syntax Definitions

service_id	An existing service ID number.
all	Applies this command to all service ID numbers.
tandem	Specifies the tandem replication mode for the service.
head-end	Specifies the head-end replication mode for the service.
hybrid	Specifies the hybrid replication mode for the service. This mode uses both the head-end and tandem methods.

Defaults

By default, an SPB service is configured to use the head-end mode and a VXLAN service is configured to use the hybrid mode.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When an SPB service is configured to use the head-end mode, a non-unicast packet received on an SPB access port is replicated once for each receiver in the provider backbone bridge (PBB) network using its unicast base MAC (BMAC) address.
- When an SPB service is configured to use the tandem mode, a non-unicast packet received on an SPB access port is replicated once at each node using the multicast group address.
- When configuring IP Multicast Switching (IPMS) for an SPB service, make sure the service was configured to use the head-end multicast mode; IPMS is not supported on SPB services that are configured to use the tandem mode.
- Make sure that the same multicast mode is used across all nodes for a given SPB BVLAN. Tandem nodes and head-end nodes cannot communicate with each other.
- The following multicast mode functionality is supported for VXLAN services:
  - **Tandem**: In this mode, PIM multicast routing is required to discover the neighbor nodes and assign membership to VTEP nodes that desire to be in the same multicast group. This requires the manual configuration of a multicast SDP object (an SDP configured with a multicast group address) to tunnel traffic to the other VTEP nodes that belong to the same multicast group.
  - **Head-end**: In this mode, unicast SDP objects (SDPs configured with a far-end IP address) are also manually configured to tunnel traffic to the far-end nodes. In this case, however, PIM multicast routing is not required. Any broadcast, unknown unicast, and multicast (BUM) traffic is replicated and one copy is sent to each VTEP node as specified by the unicast SDP object.
  - **Hybrid**: In this mode, traffic is tunneled from this service instance to both a group of VTEPs that belong to the same multicast group address and to the VTEP nodes that are not associated with the same multicast group address.

- Configuring a VXLAN service on an OmniSwitch 6900-V72 or OmniSwitch 6900-C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. If the hybrid mode is selected, only the head-end mode is active.
- L2 GRE tunneling services do not support multicast modes. All Broadcast, Unknown Unicast, and Multicast (BUM) traffic is replicated; a copy is sent to each far-end node over unicast SDPs (similar to the head-end multicast mode).
- This command configures the multicast mode for an existing service. However, the **multicast-mode {head-end | tandem | hybrid}** parameter is also used to specify the status at the time the service is created.

Examples

Configuring the multicast mode for an existing service:

```
-> service 100 multicast-mode hybrid
-> service 150 multicast-mode head-end
-> service all multicast-mode tandem
```

Configuring the multicast mode for a new service:

```
-> service 100 spb isid 2345 bvlan 3000 multicast-mode tandem
-> service 150 vxlan vnid 24000 multicast-mode head-end
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.

Related Commands

service spb	Configures an SPB service.
service vxlan	Configures a VXLAN service.
service description	Configures a description for the specified service.
service stats	Configures the statistics collection status for the specified service.
service vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.
service admin-state	Configures the administrative status of the specified service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcMulticastMode
```

service stats

Configures ingress and egress statistics collection for packets flowing through the service access point (SAP) or service distribution point (SDP) bindings associated with the specified service.

service {*service_id* **| all} stats {enable | disable}**

Syntax Definitions

service_id	An existing service ID number.
all	Applies this command to all service ID numbers.
enable	Administratively enables statistics gathering for the service.
disable	Administratively disables statistics gathering for the service.

Defaults

By default, statistics collection is disabled when the service is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

This command configures statistics collection for an existing service. However, the **stats {enable | disable}** parameter is also used to specify the status at the time the service is created.

Examples

Configuring statistics collection for an existing service:

```
-> service 100 stats enable
-> service all stats enable
-> service 100 stats disable
-> service all stats disable
```

Configuring statistics collection for a new service:

```
-> service 200 isid 2345 bvlan 3000 stats enable
-> service 200 isid 3456 bvlan 2000 stats disable
-> service 300 vxlan vnid 24000 stats enable
-> service 300 vxlan vnid 24000 stats disable
-> service 400 l2gre vpnid 40 stats enable
-> service 400 l2gre vpnid 40 stats disable
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service spb	Configures an SPB service.
service vxlan	Configures a VXLAN service.
service description	Configures a description for the specified service.
service multicast-mode	Configures the multicast replication mode for the specified service.
service vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.
service admin-state	Configures the administrative status of the specified service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcStatsAdminStatus
```

service vlan-xlation

Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.

service {*service_id* **| all} vlan-xlation {enable | disable}**

Syntax Definitions

service_id	An existing service ID number.
all	Applies this command to all service ID numbers.
enable	Enables VLAN translation for the service.
disable	Disables VLAN translation for the service.

Defaults

By default, VLAN translation is disabled when the service is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Enabling VLAN translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled.
- Mixing switches with VLAN translation enabled on some and disabled on other switches in the same network is not recommended.
- This command configures the VLAN translation status for an existing service. However, the **vlan-xlation {enable | disable}** parameter is also used to specify the status at the time a service is created.

Examples

Configuring the status for an existing service:

```
-> service 100 vlan-translation enable
-> service all vlan-translation enable
-> service 100 vlan-translation disable
-> service all vlan-translation disable
```

Configuring the status for a new service:

```
-> service 200 isid 2345 bvlan 3000 vlan-translation enable
-> service 200 isid 3456 bvlan 2000 vlan-translation disable
-> service 300 vxlan vnid 24000 vlan-translation enable
-> service 300 vxlan vnid 24000 vlan-translation disable
-> service 400 l2gre vpnid 40 vlan-translation enable
-> service 400 l2gre vpnid 40 vlan-translation disable
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service spb	Configures an SPB service.
service vxlan	Configures a VXLAN service.
service description	Configures a description for the specified service.
service multicast-mode	Configures the multicast replication mode for the specified service.
service stats	Configures the statistics collection status for the specified service.
service admin-state	Configures the administrative status of the specified service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcSapVlanXlation
```

service admin-state

Configures the administrative status of the specified service.

service {*service_id* **| all} admin-state {enable | disable}**

Syntax Definitions

service_id	An existing service ID number.
all	Applies this command to all service ID numbers.
enable	Administratively enables the service.
disable	Administratively disables the service.

Defaults

By default, the administrative status is disabled when the service is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Disable the administrative status of the service and any associated service access points (SAPs) and service distribution points (SDPs) before attempting to remove a service.
- Disabling the administrative status does not remove the service configuration from the bridge.
- This command configures the administrative status for an existing service. However, the **admin-state {enable | disable}** parameter is also used to specify the status at the time the service is created.

Examples

Configuring the status for an existing service:

```
-> service 100 admin-state enable
-> service all admin-state enable
-> service 100 admin-state disable
-> service all admin-state disable
```

Configuring the status for a new service:

```
-> service 200 isid 2345 bvlan 3000 admin-state enable
-> service 200 isid 3456 bvlan 2000 admin-state disable
-> service 300 vxlan vnid 24000 admin-state enable
-> service 300 vxlan vnid 24000 admin-state disable
-> service 400 l2gre vpnid 40 admin-state enable
-> service 400 l2gre vpnid 40 admin-state disable
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service spb	Configures an SPB service.
service vxlan	Configures a VXLAN service.
service description	Configures a description for the specified service.
service multicast-mode	Configures the multicast replication mode for the specified service.
service stats	Configures the statistics collection status for the specified service.
service vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcAdminStatus
```

service remove-ingress-tag

Configures whether or not the customer VLAN tag is removed from ingress packets for the specified Virtual eXtensible LAN (VXLAN) or Layer 2 Generic Routing Encapsulation (L2 GRE) service.

service *service_id* **remove-ingress-tag {enable | disable}**

Syntax Definitions

service_id	An existing service ID number.
enable	Customer VLAN tag is removed from ingress packets.
disable	Customer VLAN tag is not removed from ingress packets.

Defaults

By default, this functionality is disabled when the service is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Removing the customer VLAN tag from ingress packets is particularly useful for services that may forward packets to third-party devices that require untagged packets.
- When this function is enabled, the customer VLAN tag is removed before the packet is encapsulated with a header. The packet is then untagged when the header is removed. For example:
  - The remove ingress tag function is enabled for service 10.
  - Service 10 is associated with SAP 1/2:20 (port 1/2, VLAN tag 20) and SAP 9:30 (link aggregate 9, VLAN tag 30).
  - When a customer packet with VLAN tag 20 enters port 1/2, the packet is classified for service 10 and the VLAN 20 tag is removed before the header is added to the untagged packet.
  - When a customer packet with VLAN tag 30 enters link aggregate 9, the packet is classified for service 10 and the VLAN 30 tag is removed before the header is added to the untagged packet.
- This command configures the status of the remove ingress tag functionality for an existing service. However, the **remove-ingress-tag {enable | disable}** parameter is also used to specify the status at the time a service is created.

Examples

Configuring the status for an existing service:

```
-> service 100 remove-ingress-tag enable
-> service 100 remove-ingress-tag disable
```

Configuring the status for a new service:

```
-> service 200 vxlan vnid 24000 remove-ingress-tag enable
-> service 200 vxlan vnid 24000 remove-ingress-tag disable
-> service 300 l2gre vpnid 25000 remove-ingress-tag enable
-> service 300 l2gre vpnid 25000 remove-ingerss-tag disable
```

Release History

Release 7.3.4; command was introduced.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service vxlan	Configures a VXLAN service.
service l2gre	Configures an L2 GRE service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcRemoveIngressTag
```

service vxlan udp-port

Configures the UDP destination port for all encapsulated VXLAN frames on the gateway switch. Use this command to support previous implementations of the VXLAN functionality that did not use the well-known UDP port 4789. Note that only gateway devices using the same destination UDP port number can exchange encapsulated VXLAN frames.

service vxlan udp-port {*udp_port_num* **| default}**

Syntax Definitions

udp_port_num	The UDP destination port number to use for VXLAN traffic.
default	Use the well-known UDP destination port number (4789) for VXLAN traffic.

Defaults

By default, the well-known UDP port number 4789 is used in the default VRF instance.

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32

Usage Guidelines

- Avoid using the well-known UDP ports that are already reserved by IANA for other applications.
- Changing the UDP port number on the fly might stop the VXLAN traffic until the VXLAN Tunnel End Points (VTEPs) in the network are configured with the same destination UDP port.
- Configuring a VXLAN service on an OmniSwitch 6900-V72 and OmniSwitch 6900-C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported.

Examples

```
-> service vxlan udp-port 8472
-> service vxlan udp-port default
```

Release History

Release 7.3.4; command was introduced.

Related Commands

service vxlan vrf	Configures the VRF instance for the VXLAN segment.
service vxlan	Configures a VXLAN service.
show service info	Displays the destination UDP port value applied to VXLAN traffic.

MIB Objects

```
alaSvcMgrSysTable
   alaSvcMgrVxlanDestUdpPort
```

service vxlan vrf

Configures the current VRF instance for the VXLAN gateway.

service vxlan vrf {*vrf_name* **| default}**

Syntax Definitions

vrf_name	The name of an existing VRF instance.
default	Use the default VRF instance.

Defaults

By default, the default VRF instance is used.

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32

Usage Guidelines

- Administratively disable all configured SDPs first before changing the VRF instance for the VXLAN segment.
- If the VRF instance that is associated with a VXLAN segment is removed, the VXLAN segment is automatically assigned to the default VRF instance.
- Avoid configuring the same Loopback0 address in multiple VRF' instances. Each VRF instance should have a unique Loopback0 address.
- Configuring a VXLAN service on an OmniSwitch 6900-V72 or OmniSwitch 6900-C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported.

Examples

```
-> service vxlan vrf IpVxlan
-> service vxlan vrf default
```

Release History

Release 7.3.4; command was introduced.

Related Commands

service vxlan	Configures a VXLAN service.
show service info	Displays the current VRF instance for the VXLAN network.

MIB Objects

```
alaSvcMgrSysTable
   alaSvcMgrVxlanCurrentVrf
```

service local-vrrp

Configures whether or not the customer VLAN tag is removed from VRRP packets received on SPB service access ports. When enabled, the VLAN tag is automatically removed from the VRRP packets. This is particularly useful when a switch is going to route VRRP packets using IP over SPB.

service local-vrrp {enable | disable}

Syntax Definitions

enable	Enables the TCAM rule (VLAN tag is stripped from VRRP packets received on access ports).
disable	Disables the TCAM rule (VLAN tag is not stripped from VRRP packets received on access ports).

Defaults

By default, the customer VLAN tag is removed from VRRP packets received on SPB service access ports.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- This command is a global configuration command; the status applies to all access ports on the switch.
- This functionality is enabled to facilitate the processing of VRRP packets received on service access ports on a switch that participates in an IP over SPB routing configuration. When this function is disabled, the customer VLAN tag is not removed from VRRP packets are trapped to the switch for local VRRP processing and are not routed through the IP over SPB configuration.
- When this functionality is enabled (the default), one of the following actions is required based on the switch configuration:
  - If the switch is participating in an IP over SPB routing configuration, enable VLAN translation on all access ports and associated SPB services. This ensures that the VLAN tag is added back into the VRRP packets egressing the access ports.
  - If the switch serves as a transit switch that receives VRRP traffic from another OmniSwitch or a third-party device, use the **service local-vrrp** command with the **disable** option to prevent the switch from removing the customer VLAN tag. This helps to avoid having to enable VLAN translation on every single access port and SPB service on the switch.
- When VLAN translation is enabled, a Service Access Point (SAP) with the encapsulation value set to ":all" (all tagged and untagged packets not already assigned) will not work. The ":all" encapsulation value is treated as a ":0" encapsulation value (untagged packets only; tagged packets are dropped) for VLAN translation.

Examples

```
-> service local-vrrp disable
-> service local-vrrp enable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

service access	Configures a switch port or link aggregate as an access port.
service access vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified access port.
service vlan-xlation	Configures the status of egress VLAN translation for the specified service.
show service info	Displays the Service Manager configuration for the local switch.

MIB Objects

```
alaSvcMgrSysTable
   alaSvcMgrVrrpMacTcamRuleAdminState
```

service l2gre reserved-vlan

Configures a reserved VLAN to activate L2 GRE service domain learning on an L2 GRE tunnel access switch.

service l2gre reserved-vlan *vlan_id***[-***vlan_id2***]**

no service l2gre reserved-vlan *vlan_id***[-***vlan_id2***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	A VLAN ID number to configure as an L2 GRE reserved VLAN. Use a hyphen to specify a range of VLAN IDs. The valid range is 2–4092. Up to 8 reserved VLANs can be configured.

Defaults

By default, there is no L2 GRE reserved VLAN configured for the switch.

Platforms Supported

OmniSwitch 6560

Usage Guidelines

- This command is required only on an OmniSwitch 6560 that serves as an L2 GRE tunnel access switch. A reserved VLAN is not required for other supported OmniSwitch platforms.
- If there is no reserved VLAN configured, UNP does not learn users in the L2 GRE service domain. When a reserved VLAN is created, any blocked users are then learned.
- Use the **no** form of this command to remove an L2 GRE reserved VLAN from the switch configuration. Make sure there are no L2 GRE service objects (SAP, SDP, SDP bindings) configured before attempting to remove the reserved VLAN.
- Specify a VLAN ID that does not already exist in the switch configuration. Use the **show vlan** command to display the VLAN configuration and verify the L2 GRE reserved VLAN configuration.
- The reserved VLAN is used only for L2 GRE learning purposes; other VLAN management operations do not apply to this type of VLAN.

Examples

```
-> service l2gre reserved-vlan 4000
-> service l2gre reserved-vlan 4005-4008
-> no service l2gre reserved-vlan 4000
-> no service l2gre reserved-vlan 4005-4008

-> service l2gre reserved-vlan 4008-4020
ERROR: VLAN range should be less than or equal to 8.

-> service l2gre reserved-vlan 200
ERROR: Vlan 200 exists. Can not create the vlan!
```

```
-> show vlan
 vlan    type   admin   oper    ip    mtu          name
------+-------+-------+------+------+------+-----------------
1      std       Ena     Dis   Ena    1500    VLAN 1
200    std       Ena     Dis   Dis    1500    VLAN 200
500    spb       Ena     Dis   Dis    1524    VLAN 500
4000   l2gre     Ena     Ena   Dis    1500    L2GRE RESERVED
4005   l2gre     Ena     Ena   Dis    1500    L2GRE RESERVED
4006   l2gre     Ena     Ena   Dis    1500    L2GRE RESERVED
4007   l2gre     Ena     Ena   Dis    1500    L2GRE RESERVED
4008   l2gre     Ena     Ena   Dis    1500    L2GRE RESERVED
4094   vcm       Ena     Dis   Dis    1500    VCM IPC
```

Release History

Release 8.5R4; command was introduced.
Release 8.6R1; configuring a range of L2 GRE reserved VLANs allowed.

Related Commands

show service info	Displays the Service Manager configuration for the local switch.

MIB Objects

```
alaSvcMgrSysTable
   alaSvcMgrReservedL2greVlan
```

service l2profile

Configures a Layer 2 profile that is applied to an access (customer facing) port. This profile is used to specify how to process Layer 2 control frames ingressing on the access port.

service l2profile *l2profile_name* **[stp | 802.1x | 802.3ad | 802.1ab | mvrp | gvrp | amap] [peer | drop | tunnel]**

no service l2profile *profile-name*

Syntax Definitions

l2profile_name	Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., "ALE Engineering").
stp	Specifies how to process Spanning Tree BPDU.
802.1x	Specifies how to process 802.1x control frames.
802.3ad	Specifies how to process 802.3ad control frames.
802.1ab	Specifies how to process 802.1AB control frames. To specify how to process tagged and untagged 802.1AB control frames separately, use the **service l2profile inbound 802.1ab** command.
mvrp	Specifies how to process Multiple VLAN Registration Protocol packets.
gvrp	Specifies how to process GARP VLAN Registration Protocol packets.
amap	Specifies how to process Alcatel-Lucent Enterprise Management Adjacency Protocol packets.
peer	Allows the access port to participate in the specified protocol. Control packets are not sent to the network side of the node.
drop	Discards the specified PDU.
tunnel	Tunnels the specified PDU across the provider network.

Defaults

If no parameters are specified with this command, the new profile inherits all the following protocol settings from the default profile (**def-access-profile** or **unp-def-access-profile**):

parameter	def-access-profile	unp-def-access-profile
stp	**tunnel**	**drop**
802.1x	**drop**	**peer**
802.3ad	**peer**	**peer**
mvrp	**tunnel**	**tunnel**
gvrp	**tunnel**	**tunnel**
amap	**drop**	**drop**
802.1ab	**drop**	**drop**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a Layer 2 profile. Removing the **def-access-profile** or the **unp-def-access-profile** is not allowed.
- Remove any profile associations with access ports before attempting to modify or delete the profile.
- Not all of the control protocols are currently supported with the **peer**, **tunnel**, and **drop** parameters. Use the following table to determine the parameter combinations that are supported:

Protocol	Reserved MAC	peer	drop	tunnel
STP	01-80-C2-00-00-00	no	yes	yes
802.1x	01-80-C2-00-00-03	yes	yes	yes
802.3ad	01-80-C2-00-00-02	yes	no	no
MVRP	01-80-C2-00-00-21	no	yes	yes
GVRP	01-80-C2-00-00-21	no	yes	yes
AMAP	00-20-DA-00-70-04	yes	yes	yes
802.1ab	01-80-C2-00-00-0E	yes	yes	yes

- If a user-configured Layer 2 profile is *not* associated with a service access port, then the **def-access-profile** is used to process control packets that ingress on the service access port.
- If a user-configured Layer 2 profile is *not* associated with a UNP access port, then the **unp-def-access-profile** is used to process control packets that ingress on the UNP access port.

Examples

```
-> service l2profile sap_1_profile stp drop
-> no service l2profile sap_1_profile
-> service l2profile DropL2
-> service l2profile DropL2 stp drop gvrp drop 802.1ab drop
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service access	Configures a switch port or link aggregate as an access port.
service l2profile inbound 802.1ab	Configures how tagged and untagged 802.1AB control frames are processed.
service access l2profile	Assigns a Layer 2 profile to the specified service access port.
unp l2-profile	Assigns a Layer 2 profile to the specified UNP access port.
show service l2profile	Displays the Layer 2 profile configuration information for the bridge.

MIB Objects

```
alaServiceMgrPortProfileTable
   alaServiceMgrPortProfileID
   alaServiceMgrPortProfileStpBpduTreatment
   alaServiceMgrPortProfile8021xTreatment
   alaServiceMgrPortProfile8021ABTreatment
   alaEServiceUNIProfileGvrpTreatment
   alaServiceMgrPortProfileAmapTreatment
   alaServiceMgrPortProfile8023ADTreatment
```

service l2profile inbound 802.1ab

Configures the treatment of Layer 2 tagged and untagged 802.1AB control frames that are received on access (customer facing) ports. Use this command to specify a different action (peer, drop, or tunnel) based on the tagged and untagged state of an 802.1AB control frame.

service l2profile *l2profile_name* **inbound {tagged |untagged | both} 802.1ab {peer | drop | tunnel}**

no service l2profile *profile-name*

Syntax Definitions

l2profile_name	The name of an existing or new Layer 2 profile.
tagged	The specified action is applied only to tagged 802.1AB control frames.
untagged	The specified action is applied only to untagged 802.1AB control frames.
both	The specified action is applied to both tagged and untagged 802.1AB control frames.
peer	Allows the access port to participate in the 802.1AB protocol. Control packets are not sent to the network side of the node.
drop	Discards 802.1AB PDUs.
tunnel	Tunnels 802.1AB PDUs across the provider network.

Defaults

By default, tagged and untagged 802.1AB control frames are dropped.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the specified Layer 2 profile. Remove any profile associations with access ports before attempting to modify or delete the profile.
- When only the **tagged** keyword is used, the specified action is applied to tagged traffic and the default action (**drop**) is applied to untagged traffic.
- When only the **untagged** keyword is used, the specified action is applied to untagged traffic and the default action (**drop**) is applied to tagged traffic.
- Only the **tunnel** and **drop** actions can be configured for tagged control frames.
- Only the **peer** and **drop** actions can be configured for untagged control frames.
- The treatment of 802.1AB control frames received on access ports can either be mixed (different for tagged, different for untagged) or the same for both tagged and untagged control frames. To switch between mixed and the same, set the action for tagged and untagged frames back to the default (**drop**).
- Use the **service l2profile** command to configure the treatment for other protocol control frames. This command applies only to 801.1AB frames.

Examples

```
-> service l2profile lldp-tagged inbound tagged 802.1ab tunnel
-> service l2profile lldp-untagged inbound untagged 802.1ab peer
-> service l2profile lldp-diff inbound tagged 802.1ab tunnel inbound untagged
802.1ab peer
-> service l2profile lldp-both inbound both 802.1ab drop

-> no service l2profile lldp-tagged
-> no service l2profile lldp-untagged
-> no service l2profile lldp-diff
-> no service l2profile lldp-both
```

Release History

Release 8.6R2; command introduced.

Related Commands

service l2profile	Configures a Layer 2 profile that is applied to an access port.
show service l2profile	Displays the Layer 2 profile configuration information for the bridge.

MIB Objects

```
alaServiceMgrPortProfileTable
   alaServiceMgrPortProfileID
   alaServiceMgrPortProfileStpBpduTreatment
   alaServiceMgrPortProfile8021xTreatment
   alaServiceMgrPortProfile8021ABTagTreatment
   alaServiceMgrPortProfile8021ABUnTagTreatment
   alaServiceMgrPortProfile8021ABMode
   alaServiceMgrPortProfile8023ADTreatment
   alaEServiceUNIProfileGvrpTreatment
   alaServiceMgrPortProfileAmapTreatment
   alaServiceMgrPortProfileMvrpTreatment
```

service access

Configures a switch port or link aggregate as an access port on which device traffic enters or leaves a service domain.

service access {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} [description** *port_description***]**

service access {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} no description**

no service access {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
port_description	An alphanumeric string (1–128 characters).

Defaults

parameter	default
port_description	No description

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to revert the port mode back to a regular switch port or link aggregate. Make sure the access port is not associated with any Service Access Points (SAPs) before attempting to change the port mode.
- Use the **no** form of the **description** parameter to remove only the description information from the access port. This option does not remove the access port designation, just the description text that was assigned to the port.
- Before configuring a port or link aggregate as an access port, make sure there is *no* IP interface configured for the default VLAN of the port. If there is, configuring the port as an access port is not allowed. For example, if VLAN 10 has an IP interface and is the default VLAN for port 1/1/1, then configuring port 1/1/1 as an access port is not supported.
- Access ports are required to configure a SAP. A SAP is the point at which customer traffic enters and exits the service. SAPs are not configurable on other port types.

Examples

```
-> service access port 1/1/3-10
-> service access linkagg 10-12
```

```
-> service access port 1/1/6 description "Voice Access Port"
-> service access port 2/1/6 description "L3 VPN Loopback Port"
-> service access linkagg 100 description "Server Access Port"
-> service access port 2/1/6 no description
-> no service access port 1/1/3
-> no service access linkagg 10

-> vlan 100
-> ip interface v100 address 10.10.10.1 vlan 100
-> vlan 100 members port 1/1/1 untagged
-> service access port 1/1/1
ERROR: A vlan with IP interface attached to this port is not supported!
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.2; **description** parameter added.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service l2profile	Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames that ingress on the access port.
service access l2profile	Assigns a Layer 2 profile to the specified service access port.
service access vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified access port.
show service access	Displays the access (customer-facing) port configuration for the bridge.

MIB Objects

```
alaServiceMgrPortTable
   alaServiceMgrPortID
   alaServiceMgrPortMode
   alaServiceMgrPortDescription
```

service access l2profile

Assigns an existing Layer 2 profile to the specified service access port. This profile determines how Layer 2 protocol frames received on the access port are processed.

service access {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} l2profile {default |** *profile-name***}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
default	Assigns the default profile to the specified port.
profile-name	The name of an existing Layer 2 profile.

Defaults

By default, the default Layer 2 profile (**def-access-profile**) is assigned when a port is configured as a service access port.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **default** parameter with this command to revert the associated profile back to the default profile settings.
- Specify only ports or link aggregates that are configured as service access ports. This command does not apply to network ports.
- Specify a profile name that already exists in the switch configuration.
- To assign a Layer 2 profile to a UNP access port, use the **unp l2-profile** command.

Examples

```
-> service access port 1/3 l2profile sap_1_profile
-> service access linkagg 10 l2profile sap_1_profile
-> service access port 1/3 l2profile default
-> service access linkagg 10 l2profile default
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service access	Configures a switch port or link aggregate as an access port.
service l2profile	Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.
show service l2profile	Displays the Layer 2 profile configuration information for the bridge.
show service access	Displays the access (customer-facing) port configuration for the switch.

MIB Objects

```
alaServiceMgrPortTable
   alaServiceMgrPortID
   alaServiceMgrPortMode
   alaServiceMgrPortPortProfileID
```

service access vlan-xlation

Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified access port.

service access {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} vlan-xlation {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables VLAN translation for the specified port.
disable	Disables VLAN translation for the specified port.

Defaults

By default, VLAN translation is disabled when a port or link aggregate is configured as an access port.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Specify only ports or link aggregates that are configured as service access ports. This command does not apply to interfaces configured as network ports.
- Enabling VLAN translation on a access port implicitly enables translation for all SAPs associated with that port. However, translation must also be enabled for the services associated with these SAPs. This ensures that all SAPs associated with a service will apply VLAN translation.

Examples

```
-> service access port 1/3 vlan-xlation enable
-> service access linkagg 10 vlan-xlation enable
-> service access port 1/3-10 vlan-xlation disable
-> service access linkagg 10-15 vlan-xlation disable
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service access	Configures a switch port or link aggregate as an access port.
service vlan-xlation	Configures the status of egress VLAN translation for the specified service.
show service access	Displays the access (customer-facing) port configuration for the switch.

MIB Objects

```
alaServiceMgrPortTable
   alaServiceMgrPortID
   alaServiceMgrPortMode
   alaServiceMgrPortVlanXlation
```

service sap

Configures a Service Access Point (SAP) by associating a SAP ID with a Shortest Path Bridging (SPB) service, a Virtual eXtensible LAN (VXLAN) service, or a Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel service. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of network traffic to map to the associated service.

This section describes the base command along with the other optional command keywords that are used to configure SAP parameter values. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default value.

service *service_id* **sap {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**
[*sap_id***]**
[description *desc_info***]**
[trusted | un-trusted [*priority***]]**
[stats {enable | disable}]
[admin-state {enable | disable}]

no service *service_id* **sap {port** *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} [***sap_id***]**

Syntax Definitions

service_id	An existing SPB, VXLAN, or L2 GRE service ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
sap_id	The SAP ID (chassis/slot/port:encapsulation). Refer to the table in the "Usage Guidelines" section of this command page for a list of encapsulation values to select for the SAP ID.

Defaults

When a SAP is created without specifying any optional parameter values, the SAP is created with the following defaults:

parameter	default
:0 | :all | :*qtag* | *:outer_qtag.inner_qtag*	**:0** (null - untagged traffic)
description *desc_info*	No description added
trusted | un-trusted [*priority***]**	**trusted**
stats enable | disable	**disable**
admin-state enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a SAP from the specified service.
- To define the SAP ID that will be associated with the SPB or VXLAN service, enter the access port or link aggregate number followed by one of the following encapsulation values (for example, service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID):

SAP ID Encapsulation	Customer Traffic Forwarded by the SAP
:0	Specifies a null encapsulation value for the SAP. All untagged traffic is mapped to the SAP; tagged traffic is dropped.
:all	Specifies a wildcard SAP. All tagged and untagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
*:qtag***[-***qtag2***]**	Specifies a VLAN ID tag for ingress traffic on the access port. Only traffic with this 802.1Q tag is mapped to the SAP. Use a hyphen to specify a range of VLAN IDs (21-30).
:*outer_qtag.inner_qtag*	Specifies an outer VLAN ID tag and an inner VLAN tag for ingress traffic on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.

- The **:all** (wild card) parameter is also configurable as the inner tag value for double-tagged packets (for example, “10:all” specifies double-tagged packets with an outer tag equal to VLAN 10 and an inner tag with any VLAN ID value).
- When VLAN translation is enabled, a Service Access Point (SAP) with the encapsulation value set to ":all" (all tagged and untagged packets not already assigned) will not work. The ":all" encapsulation value is treated as a ":0" encapsulation value (untagged packets only; tagged packets are dropped) for VLAN translation.
- Specify only ports or link aggregates that are configured as service access ports (see **service access**). This command does not apply to network ports.
- Configuring SAPs with different encapsulation types for the same access port is allowed.
- When specifying a range of VLAN IDs with this command on an OmniSwitch 6900-Q32 or OmniSwitch 6900-X72, consider the following guidelines:
  - Each service access port supports a maximum of 8 SAPs that are created with a range of VLANs.
  - A total of 255 service access ports can support a range of VLANs at any given time.
  - The range of VLANs specified for the SAPs of a service access port cannot overlap each other.
  - For double-tagged SAPs, separate range commands can be specified for both outer and inner VLAN tags.
  - The outer VLAN range space is shared with the same space as QTAG SAP. The combined limit is 8 unique ranges per service access port. This is in addition to the 8 unique inner VLAN range per service access port.
- Configuring a VXLAN service on an OmniSwitch 6900-V72 or OmniSwitch 6900-C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. If the hybrid mode is selected, only the head-end mode is active.

- When configuring a SAP for an L2 GRE tunnel, consider the following:
  - A SAP is manually configured on a tunnel aggregation switch through the **service sap** command.
  - Configuring a SAP on a tunnel aggregation switch is supported on the OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, OmniSwitch 6900-X72, and OmniSwitch 9900.
  - A SAP is dynamically created on a tunnel access switch based on the L2 GRE tunnel service parameters mapped to the UNP profile when qualifying device traffic is assigned to the profile. Refer to Chapter 39, "Access Guardian Commands," for information about how to configure a UNP L2 GRE service profile.

Examples

```
-> service 100 sap port 1/1/1:0
-> service 100 sap port 1/1/1:50 description “Server1 to VXLAN10 SAP”
-> service 100 sap port 1/2/10:100.200 admin-state enable
-> service 100 sap port 1/2/10:500.all untrusted stats enable
-> service 100 sap linkagg 5:10
-> service 200 sap linkagg 2:20.30
-> service 200 sap linkagg 9:all untrusted 3 stats enable admin-state enable
-> no service 100 sap port 1/1/1:50 description
-> no service 100 sap port 1/2/10:100.200
-> no service 200 sap linkagg 9:all

-> service 10 sap port 1/1/11-20:21-30 description "SAPs on ports 1/1/11 to 1/1/20
with tag 21 to 30"
-> service 20 sap linkagg 1-10:100 un-trusted description "Untrusted SAPs for lag
1-10 with tag 100"
-> service 30 sap port 1/1/2:10-20 description "SAP on port 1/1/2 with only one VP
for tag 10-20"
-> service 30 sap linkagg 11:10-20 description "SAP on lag 11 with only one VP for
tag 10-20"
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, link aggregates, and VLAN ID tags added; VXLAN service support added).
Release 8.4.1.R02; support for L2 GRE tunnel services added.

Related Commands

service sap description	Configures a description for the specified SAP ID.
service sap trusted	Configures the trust mode for the specified SAP ID.
service sap stats	Configures statistics collection for the specified SAP ID.
service sap admin-state	Configures the administrative status for the specified SAP ID.
service spb	Configures an SPB service.
service vxlan	Configures a VXLAN service.
service l2gre	Configures an L2 GRE tunnel service.
service access	Configures a service access port.
show service ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
   alaSapSvcId
   alaSapPortId
   alaSapEncapValue
   alaSapType
   alaSapDescription
   alaSapTrusted
   alaSapPriority
   alaSapStatsAdminStatus
   alaSapAdminStatus
```

service sap description

Configures a description for the specified Service Access Point (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

service *service_id* **sap {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} {:0 | :all | :**qtag**[**-*qtag2***]** | **:***outer_qtag.inner_qtag***} description** *desc_info*

no service *service_id* **sap {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} [:0 | :all | :**qtag**[**-*qtag2***]** | **:***outer_qtag.inner_qtag***] description**

Syntax Definitions

service_id	An existing SPB, VXLAN, or L2 GRE service ID number.
chassis	The chassis identifier when running in virtual chassis mode.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
*:qtag***[**-*qtag2***]**	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Use a hyphen to specify a range of VLAN IDs (21-30).
:*outer_qtag.inner_qtag*	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
desc_info	An ASCII text string up to 160 characters in length.

Defaults

By default, a description is not added when the SAP is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the description from the specified SAP.
- Specify the service ID number associated with the specified SAP ID (access port/encapsulation).

Examples

```
-> service 10 sap port 1/2:10 description “CE1 to SPB10 SAP”
-> service 13 sap linkagg 20:100.200 description “CE2 to SPB13 SAP”
```

```
-> service 15 sap port 1/11-20:21-30 description "SAPs on ports 1/11 to 1/20 with
tag 21 to 30"
-> service 30 sap port 1/2:10-20 description "SAP on port 1/2 with only one VP for
tag 10-20"
-> service 10 sap port 1/2:10 no description
-> service 13 sap linkagg 20:100.200 no description
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, linkaggs, and VLAN ID tags added; VXLAN service support added.
Release 8.4.1.R02; support for L2 GRE tunnel services added.

Related Commands

service sap	Configures a SAP by associating a SAP ID with a SPB service.
service sap trusted	Configures the trust mode for the specified SAP ID.
service sap stats	Configures statistics collection for the specified SAP ID.
service sap admin-state	Configures the administrative status for the specified SAP ID.
show service ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
   alaSapPortId
   alaSapEncapValue
   alaSapDescription
   alaSapSvcId
```

service sap trusted

Configures the trust mode for the specified Service Access Port (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

A trusted SAP can accept 802.1p values in incoming packets; an untrusted SAP will set any 802.1p values to zero in incoming packets, unless an 802.1p value is configured with this command.

service *service_id* **sap {port** *chassis/slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag* | **:***outer_qtag.inner_qtag***] {trusted | un-trusted [***priority***]}**

Syntax Definitions

service_id	An existing SPB, VXLAN, or L2 GRE service ID number.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
*:qtag***[-***qtag2***]**	Specifies a VLAN ID tag for traffic received on the access port. Only traffic with this tag is mapped to this SAP. Use a hyphen to specify a range of VLAN IDs (21-30).
:*outer_qtag.inner_qtag*	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic received on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
trusted	Allows the SAP to use the priority value obtained from tagged packets received on the SAP port. Untagged packets use the default port priority value.
un-trusted	Sets the priority value to zero for tagged and untagged packets received on the SAP. This is the priority assigned to tagged and untagged packets received on an untrusted SAP.
priority	The priority value to set for tagged and untagged packets received on an untrusted SAP. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

By default, the SAP is trusted with the priority set to best effort (zero). These default values are set when a port is configured as an access port and then associated with the SAP.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **un-trusted** and the *priority* parameter options to assign an 802.1p priority value to ingress packets processed by the SAP. When the **un-trusted** parameter is used without specifying a priority value, a value of zero is automatically assigned to the ingress packets.
- Specify the service ID number associated with the specified SAP ID (access port/encapsulation).
- Administratively disabling the SAP is not required to change the trust mode for the SAP.
- When the trust mode is changed from untrusted to trusted, the priority value is automatically set to the default best effort priority value (zero).
- Note that untagged Layer 2 control packets (for example, BPDU, GVRP, and AMAP) are always tunneled (if enabled) through the provider backbone bridge (PBB) network with the default EXP bits set to 7, so that they can arrive at the destination bridge at the highest COS queue of 7. As a result, trusted and untrusted SAPs configured on the access ports will not affect the Layer 2 control packets ingressing on the access ports.
- Configuring the trust mode on an access port is not allowed. These settings are configured for the SAP to which the access port is associated.
- Configuring the trust mode for a SAP is not supported on the OmniSwitch 9900.

Examples

```
-> service 10 sap port 1/1/2:10 trusted
-> service 13 sap linkagg 20 trusted
-> service 10 sap port 1/1/2:10 un-trusted
-> service 13 sap linkagg 20 un-trusted 5
-> service 20 sap linkagg 1-10:100 un-trusted
-> service 30 sap linkagg 11:10-20 trusted
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, linkaggs, and VLAN ID tags added; VXLAN service support added.
Release 8.4.1.R02; support for L2 GRE tunnel services added.

Related Commands

service sap	Configures a SAP by associating a SAP ID with a SPB service.
service sap description	Configures a description for the specified SAP ID.
service sap stats	Configures statistics collection for the specified SAP ID.
service sap admin-state	Configures the administrative status for the specified SAP ID.
show service ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
   alaSapPortId
   alaSapEncapValue
   alaSapTrusted
   alaSapPriority
   alaSapSvcId
```

service sap stats

Configures ingress and egress statistics collection for packets flowing through the specified SAP ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

service *service_id* **sap {port** *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} {:0 | :all |** *:qtag***[-***qtag2***] | :***outer_qtag.inner_qtag***} stats {enable | disable}**

Syntax Definitions

service_id	An existing SPB, VXLAN, or L2 GRE service ID number.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
*:qtag***[-***qtag2***]**	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Use a hyphen to specify a range of VLAN IDs (21-30).
:*outer_qtag.inner_qtag*	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
enable	Enables statistics collection for the SAP.
disable	Disables statistics collection for the SAP.

Defaults

By default, statistics collection is disabled for the SAP.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Specify the service ID number associated with the specified SAP ID (access port/encapsulation).

Examples

```
-> service 100 sap port 1/1/2:10 stats enable
-> service 101 sap linkagg 20:all stats enable
-> service 100 sap port 1/1/2:10 stats disable
-> service 101 sap linkagg 20:all stats disable
-> service 10 sap port 1/1/11-20:21-30 stats enable
```

```
-> service 30 sap linkagg 11:10-20 stats disable
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, linkaggs, and VLAN ID tags added; VXLAN service support added.
Release 8.4.1.R02; support for L2 GRE tunnel services added.

Related Commands

service sap	Configures a SAP by associating a SAP ID with a SPB service.
service sap description	Configures a description for the specified SAP ID.
service sap trusted	Configures the trust mode for the specified SAP ID.
service sap admin-state	Configures the administrative status for the specified SAP ID.
show service ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
   alaSapPortId
   alaSapEncapValue
   alaSapStatsAdminStatus
   alaSapSvcId
```

service sap admin-state

Configures the administrative status for the specified Service Access Point (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

service *service_id* **sap {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} {:0 | :all |** *:qtag***[**-*qtag2***] | :***outer_qtag.inner_qtag***} admin-state {enable | disable}**

Syntax Definitions

service_id	An existing SPB, VXLAN, or L2 GRE service ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
*:qtag***[**-*qtag2***]**	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Use a hyphen to specify a range of VLAN IDs (21-30
:*outer_qtag.inner_qtag*	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
enable	Enables the administrative status for the SAP.
disable	Disables the administrative status for the SAP.

Defaults

By default, the administrative status of the SAP is enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Specify the service ID number associated with the specified SAP ID (access port/encapsulation).
- Disabling the SAP administrative status does not remove the SAP configuration from the bridge.
- If an access port goes down, all SAPs associated with that port are operationally taken down as well.

Examples

```
-> service 10 sap port 1/2:10 admin-state enable
-> service 13 sap linkagg 20 admin-state enable
-> service 10 sap port 1/2:10 admin-state disable
-> service 13 sap linkagg 20 admin-state disable
-> service 10 sap port 1/11-20:21-30 admin-state enable
-> service 30 sap linkagg 11:10-20 admin-state disable
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, linkaggs, and VLAN ID tags added; VXLAN service support added.
Release 8.4.1.R02; support for L2 GRE tunnel services added.

Related Commands

service sap	Configures a SAP by associating a SAP ID with a SPB service.
service description	Configures a description for the specified SAP ID.
service sap trusted	Configures the trust mode for the specified SAP ID.
service sap stats	Configures statistics collection for the specified SAP ID.
show service ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
   alaSapPortId
   alaSapEncapValue
   alaSapAdminStatus
   alaSapSvcId
```

service sdp vxlan

Configures a Service Distribution Point (SDP) for Virtual eXtensible LAN (VXLAN) traffic. This type of SDP is used to tunnel unicast or multicast traffic between VXLAN Tunnel End Points (VTEPs). Configuring an SDP is automatically done for Shortest Path Bridging (SPB) services; this command is only for VXLAN services.

service sdp *sdp_id* **vxlan {far-end** *ip_address* **| multicast-group** *mc_group_address***} [ttl {***ttl_num* **| default}] [description** *desc_info***] [admin-state {enable | disable}]**

no service sdp *sdp_id* **[description]**

Syntax Definitions

sdp_id	The ID number to assign to the SDP object.
ip_address	The IP address of the Loopback0 interface for the far-end VTEP node. The Loopback0 address is required on every VTEP node.
mc_group_address	The multicast IP address of the group to which this service will join. *This parameter is not supported on an OmniSwitch 6900-V72* or an OmniSwitch 6900-C32.
ttl_num	A Time-to-Live (TTL) value that is inserted into the TTL field of the IP header when the VXLAN encapsulated frames are sent from this node. The valid range is 1–255.
default	Sets the TTL value to the default value of 64.
desc_info	An ASCII text string up to 160 characters in length.
enable	Enables the administrative status of the SDP.
disable	Disables the administrative status of the SDP.

Defaults

parameter	default
ttl {default | *ttl_num***}**	64
description *desc_info*	No description.
admin-state {enable | disable}	enable

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to delete the SDP object, only if the SDP is not bound to any services. If the **description** parameter is specified with the **no** form, then only the description information is removed from the SDP.
- When the **far-end** option is used, this command specifies a single destination unicast IP address that identifies the far-end VTEP node to which the SDP will tunnel traffic. This IP address is the Loopback0 address configured on every VTEP node. The SDP is then bound to a VXLAN service to

direct one-way VXLAN encapsulated traffic to that single far-end node. This object is similar to the unicast SDP in SPB.

- When the **multicast-group** option is used, this command specifies the multicast group address to which all broadcast, unknown unicast, and multicast (BUM) traffic is sent to the VTEP nodes that subscribe to the PIM multicast group will receive this type of traffic. In this mode, the **ttl** parameter value is included in the IP header of the VXLAN encapsulation header:
- If the IP address of a VTEP node is learned, thus creating a dynamic unicast SDP through the discovery process, the unicast traffic is sent to the VTEP node that is associated with that learned IP address. This object is similar to multicast SDP in SPB.
- The administrative status of the VXLAN SDP affects all SDP bindings that are bound to this object.
- Configuring a VXLAN service on an OmniSwitch 6900-V72 or OmniSwitch 6900-C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. As a result, creating an SDP with a multicast group address is also not supported (tandem mode services are bound to multicast SDPs).

Examples

```
-> service sdp 10 vxlan multicast-group 224.2.1.1 ttl 20 description "PIM Group
224.2.1.1"
-> service sdp 10 ttl 5
-> service sdp 20 far-end 10.10.10.2 description "Unicast to NodeB"
-> service sdp 20 admin-state disable
-> no service sdp 10 description
-> no service sdp 10
```

Release History

Release 7.3.4; command was introduced.

Related Commands

service bind-sdp	Binds VXLAN services to VXLAN SDPs.
service vxlan	Configures a VXLAN service.
show service sdp	Displays the SDP configuration for the switch.
show service bind-sdp	Displays the service-to-SDP binding configuration for the switch.

MIB Objects

```
alaSdpInfoTable
   alaSdpId
   alaSdpRowStatus
   alaSdpSvcType
   alaSdpFarEndIpAddress
   alaSdpDescription
   alaSdpAdminStatus
   alaSdpAllocationType
   alaSdpDynamicType
   alaSdpAdminTTL
```

service sdp l2gre

Configures a Service Distribution Point (SDP) for Layer 2 Generic Routing Encapsulation (L2 GRE) traffic. This type of SDP is used to tunnel encapsulated GRE traffic between two L2 GRE tunnel end points. Manual configuration of an L2 GRE SDP is required on a switch serving as a tunnel aggregation switch.

service sdp *sdp_id* **l2gre far-end** *ip_address* **[ttl {***ttl_num* **| default}] [description** *desc_info***] [admin-state {enable | disable}]**

no service sdp *sdp_id* **[description]**

Syntax Definitions

sdp_id	The ID number to assign to the SDP object.
ip_address	The IP address of the Loopback0 interface for the far-end Guest Tunnel access switch. The Loopback0 address is required on every Guest Tunnel endpoint.
ttl_num	A Time-to-Live (TTL) value that is inserted into the TTL field of the GRE header when the GRE encapsulated frames are sent from this node. The valid range is 1–255.
default	Sets the TTL value to the default value of 64.
desc_info	An ASCII text string up to 160 characters in length.
enable	Enables the administrative status of the SDP.
disable	Disables the administrative status of the SDP.

Defaults

parameter	default
ttl {default | *ttl_num***}**	64
description *desc_info*	No description.
admin-state {enable | disable}	enable

Platforms Supported

OmniSwitch 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- Use the **no** form of this command to delete the SDP object, only if the SDP is not bound to any services. If the **description** parameter is specified with the **no** form, then only the description information is removed from the SDP.
- The **far-end** IP address value specifies a single destination unicast IP address that identifies the far-end L2 GRE tunnel access switch to which the SDP will tunnel traffic. This IP address is the Loopback0 interface address configured on every tunnel end point. The SDP is then bound to an L2 GRE service to direct one-way GRE encapsulated traffic to that single far-end tunnel access switch. This object is

similar to the unicast SDP in SPB, however, multicast SDPs are not configurable for L2 GRE tunneling.

- The administrative status of the L2 GRE SDP affects all SDP bindings that are bound to this object.
- When L2 GRE automatic SDP discovery is enabled (the default), manual configuration of the SDP and SDP binding is not required on the L2 GRE tunnel aggregation switch (see the **service l2gre auto-discover** command for more information).

Examples

```
-> service sdp 20 l2gre far-end 192.168.0.10 admin-state enable description "Guest
SDP to access switch 192.168.0.10"
-> service sdp 20 ttl 5
-> service sdp 20 admin-state disable
-> no service sdp 20 description
-> no service sdp 20
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

service bind-sdp	Binds VXLAN services to VXLAN SDPs.
service l2gre	Configures an L2 GRE tunnel service.
show service sdp	Displays the SDP configuration for the switch.
show service bind-sdp	Displays the service-to-SDP binding configuration for the switch.

MIB Objects

```
alaSdpInfoTable
   alaSdpId
   alaSdpSvcType
   alaSdpCreationOrigin
   alaSdpFarEndIpAddress
   alaSdpDescription
   alaSdpAdminStatus
   alaSdpAdminTTL
   alaSdpRowStatus
```

service bind-sdp

Configures the binding of a Virtual eXtensible LAN (VXLAN) service or a Layer 2 Generic Encapsulation Routing (L2 GRE) tunnel service to a Service Distribution Point (SDP).

service *service_id* **bind-sdp** *sdp_id1* **[***sdp_id2 sdp_id3* **...] [description** *desc_info***]**

service *service_id***[-***service_id2***] bind-sdp** *sdp_id* **[description** *desc_info***]**

no service *service_id* **bind-sdp** *sdp_id* **[description]**

Syntax Definitions

*service_id***[-***service_id2***]**	An existing VXLAN service ID or an L2 GRE tunnel service ID to bind to the SDP. Use a hyphen to specify a range of services to bind to the SDP.
sdp_id	An existing SDP ID number to bind to the service. Use a space to specify additional SDP IDs to bind to the specified service (for example, 10 20 30 40 50).
desc_info	An ASCII text string up to 160 characters in length.

Defaults

parameter	default
description *desc_info*	No description.

Platforms Supported

OmniSwitch 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to delete the SDP binding. If the **description** parameter is specified with the **no** form, then only the description information is removed from the SDP binding.
- There is no control of the SDP administrative status; this type of service object is always enabled.
- Only static SDPs (created with an SDP ID between 1–32767) can be manually bound to a VXLAN service or an L2 GRE tunnel service; otherwise, an error message is returned.
- When configuring an SDP binding for a VXLAN service, consider the following:
  - VXLAN is only supported on the OmniSwitch 6900-V72, OmniSwitch 6900-C32, OmniSwitch 6900-Q32, and OmniSwitch 6900-X72.
  - An SDP binding is defined to allow VXLAN traffic to reach other nodes in the same group (multicast SDP) or reach a single node (unicast SDP).
  - A tandem mode VXLAN service can be bound only to one multicast SDP (not supported on an OmniSwitch 6900-V72 or OmniSwitch 6900-C32).
  - A head-end mode VXLAN service can be bound only to unicast SDPs.
  - A hybrid mode service can be bound with one multicast SDP for a group of member VTEPs and

with many unicast SDPs for VTEPs that do not participate in a multicast group.

- On an OmniSwitch 6900-V72 and OmniSwitch 6900-C32, only head-end mode VXLAN services are supported. As a result, creating an SDP bind for a tandem mode service is not supported on this platform. If the service is configured to use the hybrid multicast mode, then the service can only be bound to a unicast SDP.

- When configuring an SDP binding for an L2 GRE tunnel service, consider the following:
  - An SDP and SDP binding is defined on a tunnel aggregation switch to allow L2 GRE tunnel traffic to reach a single tunnel access switch (unicast SDP).
  - One SDP and SDP binding is configured for each tunnel access switch that will tunnel traffic to the tunnel aggregation switch.
  - When L2 GRE automatic discovery is enabled (the default), manual configuration of the SDP and SDP binding is not required on the L2 GRE tunnel aggregation switch (see the **service l2gre auto-discover** command for more information).

Examples

```
-> service 1 bind-sdp 10 description "Bind to PIM Group 224.2.1.1"
-> service 2 bind-sdp 20 description "Unicast Bind to 1.1.1.20 VTEP"
-> service 4 bind-sdp 30 description “Unicast Bind to 10.2.2.1 Guest Access Switch:
-> service 5 bind-sdp 40 50 60 70 80 90
-> service 1-100 bind-sdp 10 description "Bind Services 1-100 to PIM Group
225.2.1.1"
-> service 200-250 bind-sdp 20 description "Bind Services 200-250 to 1.1.1.20 VTEP"
-> service 300-350 bind-sdp 30 description “Bind Services 300-350 to 10.2.2.1 Guest
Access Switch”
-> no service 1 bind-sdp 10 description
-> no service 2 bind-sdp
```

Release History

Release 7.3.4; command was introduced.
Release 8.4.1.R02; support for binding L2 GRE tunnel services to unicast SDPs added.

Related Commands

service sdp vxlan	Manually configures a VXLAN SDP (multicast or unicast)
service sdp l2gre	Manually configures an L2 GRE unicast SDP.
service vxlan	Configures a VXLAN service.
service l2gre	Configures an L2 GRE tunneling service.
show service sdp	Displays the SDP configuration for the switch.
show service bind-sdp	Displays the service-to-SDP binding configuration for the switch.

MIB Objects

```
alaSdpBindTable
   alaSdpBindId
   alaSdpBindCreationOrigin
   alaSdpBindSvcType
   alaSdpBindAdminStatus
   alaSdpBindStatsAdminStatus
   alaSdpBindMode
   alaSdpBindFarEndIpAddress
   alaSdpBindVnid
   alaSdpBindDescription
   alaSdpBindRowStatus
```

service l2gre auto-discover

Configures the status of L2 GRE automatic SDP discovery on a tunnel aggregation switch. When enabled, the switch discovers the SDPs of remote tunnel end points for a configured L2 GRE service. Once discovered, the switch will dynamically create local SDP and SDP bindings for the remote tunnel end points of the L2 GRE service.

service l2gre auto-discover {enable | disable}

Syntax Definitions

enable	Enables automatic discovery of L2 GRE edge switches.
disable	Disables automatic discovery of L2 GRE edge switches.

Defaults

By default, automatic discovery is enabled on an L2 GRE tunnel aggregation switch.

Platforms Supported

OmniSwitch 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- When L2 GRE automatic discovery is enabled (the default), the detection of SDPs for remote tunnel end points is based on the traffic received from these end points. If the destination IP address of the remote traffic is the IP address of the local Loopback0 interface and the VPNID of the traffic matches the VPNID of a local L2 GRE service, an SDP and SDP binding is dynamically created for the remote tunnel end point.
- When L2 GRE automatic discovery is disabled, manual configuration of an SDP and SDP binding for a remote tunnel end point is required using the **service sdp l2gre** and **service sdp-bind** commands.
- L2 GRE automatic discovery on the tunnel aggregation switch is similar to how tunnel access switches automatically define unicast SDPs to the aggregation switch.

Examples

```
-> service l2gre auto-discover disable
-> service l2gre auto-discover enable
```

Release History

Release 8.5R2; command was introduced.

Related Commands

service sdp l2gre	Configures an SDP for L2 GRE tunnel traffic.
service bind-sdp	Configures the binding of an L2 GRE tunnel service to an SDP
show service info	Displays the Service Manager configuration for the local switch.

MIB Objects

```
alaSvcMgrSysTable
   alaSvcMgrSdpAutoCreateAdminState
```

service rfp local-endpoint

Configures a local end point for an SPB Remote Fault Propagation (RFP) domain. Creating a local RFP end point identifies the local switch as a Maintenance End Point (MEP) in the RFP domain.

service rfp *rfp_id* **local-endpoint** *lep_id* **[admin-state {enable | disable}] [ccm-interval {interval100ms | interval1s** | **interval10s** | **interval1m** | **interval10m | interval-invalid}] [level** *number***] type spb**

no service rfp *rfp_id* **[local-endpoint** *lep_id***]**

Syntax Definitions

rfp_id	A unique numerical value to identify an RFP domain that maps to a reserved OAM domain. The valid RFP ID range is 1–32767.
lep_id	A numerical value to identify an end point of the specified RFP domain ID on the local switch. The valid range is 1–8191. This value serves as the virtual UP MEP ID for the RFP end point.
enable	Administratively enables the local end point.
disable	Administratively disables the local end point.
interval100ms	Send a Continuity Check Messages (CCM) every 100 milliseconds.
interval1s	Send a CCM every 1 second.
interval10s	Send a CCM every 10 seconds.
interval1m	Send a CCM every minute.
interval10m	Send a CCM every 10 minutes.
interval-invalid	Send a CCM by a MEP.
number	A unique numerical value to assign as the OAM domain level for the RFP domain. The valid range is 0-7.

Defaults

When a local end point is created for an RFP domain without specifying any of the optional parameter values, the end point is created with the following default values:

parameter	default
enable | disable	**enable**
ccm-interval	**interval1s**
number	7

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of this command to remove the RFP domain configuration from the switch (for example, **no service rfp 1**). To remove the local end point ID only, use the **no** form of this command with the **local-endpoint** parameter (for example, **no service rfp local-endpoint**).

- An RFP domain consists of a local end point configured with this command and a remote end point list configured with the **service rfp remote-endpoint** command. An SPB service is bound to the remote end point list to identify the Service Access Point (SAP) to monitor.
- The local end point ID number identifies local BEB devices in the RFP domain; this is also the number used as the virtual UP MEP ID.
- Creating more than one RFP domain with the same domain level value is not allowed. Up to eight RFP domains are allowed as long as they each are created with a different level number. Each RFP domain created counts towards the maximum limit of Ethernet OAM domains allowed.
- When this command is used to create an RFP end point, the switch automatically creates the following reserved Ethernet OAM elements that are mapped to each RFP domain:
  - Maintenance Domain (MD) named “RFP_OVER_SPB_DOMAIN_LEVEL7”, where the level number is the value specified with this command. Each time an RFP end point is created, a new maintenance domain is created with the level number specified with this command.
  - Maintenance Association (MA) named “RFP_OVER_SPB_ASSOCIATION”. The same MA name is used for all RFP domains.
  - A primary VLAN, where the VLAN ID used is the SPB control BVLAN. This same VLAN is used as the primary VLAN for all RFP domains.
  - Virtual UP Maintenance End Point (MEP) that will advertise CCM to the network. Each CCM contains a proprietary OUI TLV that specifies I-SID information and the state of the port associated with the I-SID. CCM packets are sent using the CCM interval value specified with this command. The local end point ID specified with this command serves as the virtual UP MEP ID.

Examples

```
-> service rfp 1000 local-endpoint 1 ccm-interval INTERVALS1s type SPB
-> service rfp 1000 local-endpoint 1 admin-status enable
-> service rfp 2000 local-endpoint 1 admin-status enable ccm-interval INTERVALS1s
level 6 type SPB
-> service rfp 300 local-endpoint 40 ccm-interval INTERVALS1s type level 5 SPB
-> service rfp 300 local-endpoint 40 admin-status enable
-> no service rfp 1 local-endpoint 1000
```

Release History

Release 7.3.4; command was introduced.

Related Commands

service rfp remote-endpoint	Configures a remote end point that is associated with the local end point through the RFP ID.
show service rfp	Displays the configuration and status of RFP for SPB domains.
show service rfp configuration	Displays the RFP OAM domain configuration for the bridge.

MIB Objects

```
alaRfpSpbLocalEndPointTable
   alaRfpSpbLocalEndPointRfp
   alaRfpSpbLocalEndPoint
   alaRfpSpbLocalEndPointCcmInterval
   alaRfpSpbLocalEndPointAdminStatus
   alaRfpSpbLocalEndPointLevel
   alaRfpSpbLocalEndPointCBVlan
   alaRfpSpbLocalEndPointMaintDomain
   alaRfpSpbLocalEndPointMaintAssociation
```

service rfp remote-endpoint

Configures a remote end point list for an SPB Remote Fault Propagation (RFP) domain. The list consists of the MEP IDs on remote BEBs and local SPB service ID numbers. This command triggers the sending of a Continuity Check Message (CCM) to advertise the status of the specified local SPB services to the specified remote MEP IDs.

service rfp *rfp_id* **remote-endpoint** *rep_id* **service-id** *service_id***[-***service_id2***]**

no service rfp *rfp_id* **remote-endpoint** *rep_id* **[service-id** *service_id***[-***service_id2***]]**

Syntax Definitions

rfp_id	An existing RFP ID number.
rep_id	A numerical value to identify the MEP ID of a remote BEB. The valid range is 1–8191.
*service_id***[-***service_id2***]**	An existing SPB service ID to bind to the RFP domain. Use a hyphen to specify a range of SPB services (for example, 10-12 specifies services 10, 11, and 12).

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of this command to remove the RFP end point or an SPB service ID from the end point list.
- To identify a BEB as a participating member of an RFP domain, first configure a local RFP end point with the **service rfp local-endpoint** command to create the RFP domain ID then use this command to configure the remote end point. Both types of end points use the same RFP ID, but the RFP ID specified for the remote end point must already exist.
- The MEP ID specified with this command is the end-point ID configured on the remote BEB using the **service rfp local-endpoint** command.
- One or more SPB services are bound to the RFP remote end point to identify the Service Access Point (SAP) to monitor within the RFP domain. An SPB service is associated with an SPB service instance ID (I-SID); the service is then associated with a SAP. A SAP binds together the service and the access port on which device traffic enters the SPB service domain.
- Each SPB service bound to an RFP domain identifies the SAP information (such as access port status and I-SID) that is advertised in the proprietary TLV of CCM packets. Each CCM may contain information for multiple SPB services.
- Although binding multiple SPB services to an RFP domain is allowed, monitoring SAPs associated with only one SPB service is recommended.

Examples

```
-> service rfp 1000 remote-endpoint 2 service-id 10-14
-> service rfp 1000 remote-endpoint 3 service-id 20
-> no service rfp 1000 remote-endpoint 2 service-id 10
-> no service rfp 1000 remote-endpoint 2
-> no service rfp 1000

Example when the RFP ID does not exist because a local end point with that ID was
not created:
-> service rfp 2000 remote-endpoint 2 service-id 10
ERROR: RFP Domain (2000) does not exist
```

Release History

Release 7.3.4; command was introduced.

Related Commands

service rfp local-endpoint	Configures a local end point that is associated with the remote end point through the RFP ID.
show service rfp	Displays the configuration and status of RFP for SPB domains.
show service rfp configuration	Displays the RFP OAM domain configuration for the bridge.

MIB Objects

```
alaRfpSpbRemoteEndPointTable
   alaRfpSpbRemoteEndPointRfp
   alaRfpSpbRemoteEndPoint
   alaRfpSpbRemoteEndPointServiceID
   alaRfpSpbRemoteEndPointStatus
   alaRfpSpbRemoteEndPointSystemName
   alaRfpSpbRemoteEndPointISID
   alaRfpSpbRemoteEndPointBVlan
```

show service l2profile

Displays the Layer 2 profile configuration information for the bridge. This type of profile is applied to access (customer-facing) ports and specifies how to process Layer 2 protocol frames received on this type of port.

show service l2profile [*profile_name***]**

Syntax Definitions

profile_name	An existing Layer 2 profile name. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

Defaults

By default, all profiles are displayed if a profile name is not specified with this command.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *profile-name* parameter to display information for a specific profile. Entering a profile name is case sensitive.
- If there are no profiles configured for the bridge, this command will still display the information for the default profiles (def-access-profile and unp-def-access-profile). These profiles are applied to service access ports that are not associated with a specific profile.
- An asterisk (*) appears after a profile name when the profile is assigned to UNP access ports.

Examples

```
-> show service l2profile
Legend: (*) in-use by UNP
                                                                    802.1AB 802.1AB 802.1AB
   Profile Name          STP   802.1X  802.3AD  MVRP    GVRP    AMAP   Both   Tagged Untagged
----------------------+-------+-------+-------+-------+-------+-----+-------+-------+--------
def-access-profile     tunnel  drop    peer    tunnel  tunnel  drop   drop     -       -
DropL2                 drop    drop    drop    tunnel  drop    drop   drop     -       -
lldp-tag-untag         tunnel  drop    peer    tunnel  tunnel  drop     -    tunnel  drop
lldp-tunnel            tunnel  drop    peer    tunnel  tunnel  drop   tunnel   -       -
unp-def-access-profile drop    peer    peer    tunnel  tunnel  drop   drop     -       -

->show service l2profile DropL2
Legend: (*) in-use by UNP
                                                                    802.1AB 802.1AB 802.1AB
   Profile Name          STP   802.1X  802.3AD  MVRP    GVRP    AMAP   Both   Tagged Untagged
----------------------+-------+-------+-------+-------+-------+-----+-------+-------+--------
DropL2                 drop    drop    drop    tunnel  drop    drop   drop     -       -
```

output definitions

Profile Name	The name of the Layer 2 profile.
Stp	Indicates how Spanning Tree traffic control packets are processed.
802.1x	Indicates how IEEE 802.1x control packets are processed.
802.3ad	Indicates how IEEE 802.3ad control packets are processed.
MVRP	Indicates how Multiple VLAN Registration Protocol packets are processed.
GVRP	Indicates how GARP VLAN Registration Protocol packets are processed.
AMAP	Indicates how Alcatel-Lucent Enterprise Mapping Adjacency Protocol packets are processed.
802.1AB Both	Indicates how tagged *and* untagged IEEE 802.1AB control packets are processed.
802.1AB Tagged	Indicates how tagged IEEE 802.1AB control packets are processed.
802.1AB Untagged	Indicates how untagged IEEE 802.1AB control packets are processed.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1; Layer 2 profiles for UNP access ports included in the output display.
Release 8.4.1.R02; L2 GRE tunnel service support added.
Release 8.6R2; “802.1AB Both”, “802.1AB Tagged”, and “802.1AB Untagged” fields added.

Related Commands

service l2profile	Configures a Layer 2 profile that is applied to a service access port.
service l2profile inbound 802.1ab	Configures how tagged and untagged 802.1AB control frames are processed.
service access l2profile	Assigns an existing Layer 2 profile to the specified service access port
unp l2-profile	Assigns an existing Layer 2 profile to the specified UNP access port
show service access	Displays the access (customer-facing) port configuration for the bridge.

MIB Objects

```
alaServiceMgrPortProfileTable
   alaServiceMgrPortProfileID
   alaServiceMgrPortProfileStpBpduTreatment
   alaServiceMgrPortProfile8021xTreatment
   alaServiceMgrPortProfile8021ABTreatment
   alaServiceMgrPortProfileGvrpTreatment
   alaServiceMgrPortProfileAmapTreatment
   alaServiceMgrPortProfile8023ADTreatment
   alaServiceMgrPortProfileMvrpTreatment
   alaServiceMgrPortProfile8021ABTagTreatment
   alaServiceMgrPortProfile8021ABUnTagTreatment
   alaServiceMgrPortProfile8021ABMode
```

show service access

Displays the access (customer-facing) port configuration for the bridge.

show service access [port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]] [sap]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
sap	Displays the Service Access Points (SAPs) associated with the specified access port.

Defaults

By default, all service access ports are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **port** and **linkagg** parameters to display the configuration for a specific port or link aggregate.
- Use the **sap** parameter to display the SAPs associated with the specified port.

Examples

```
-> show service access
Port     Link  SAP     SAP   Vlan
Id      Status Type    Count Xlation L2Profile              Description
-------+------+-------+-=---+-------+----------------------+-----------------------
1/11    Up     Manual  100   N       def-access-profile
1/12    Up     Manual  100   N       def-access-profile
1/13    Down   Dynamic 100   N       unp-def-access-profile UNP Dynamic Access Port
1/14    Down   Manual  100   N       def-access-profile

Total Access Ports: 4

-> show service access port 1/13
Port     Link  SAP     SAP   Vlan
Id      Status Type    Count Xlation L2Profile              Description
-------+------+-------+-=---+-------+----------------------+-----------------------
1/13    Down   Dynamic 100   N       unp-def-access-profile UNP Dynamic Access Port

Total Access Ports: 1
```

output definitions

Port Id	The access port number or link aggregate ID number.
Link Status	The status of the link connection to the access port (**Up** or **Down**).
SAP Type	Whether or not the SAP associated with the access port was created statically or dynamically (**Manual** or **Dynamic**).
SAP Count	The number of service access points (SAPs) that are associated with the access port.
VLAN Xlation	Whether or not VLAN translation is enabled on the access port.
L2Profile	The name of the Layer 2 profile associated with the access port. Configured through the **service l2profile** command.
Description	An optional description configured for the access port. By default, the description is blank.

```
-> show service access port 1/23 sap
Legend: * denotes a dynamic object
                                                                  Vlan
Identifier       Adm  Oper Stats T:P  ServiceId   Isid/Vnid Xlation Sap Description
---------------+----+----+-----+----+-----------+---------+-------+---------------
sap:1/1/23:0       Down Down  N    Y:x  20          1500        N      -
sap:1/1/23:all     Up   Down  N    N:3  10          2300        N      VXLAN SAP
sap:1/1/23:9.10    Down Down  N    Y:x  20           200        N      L2GRE SAP

Total SAPs: 3
```

output definitions

Identifier	The SAP identifier, which consists of the access port and encapsulation value.
Adm	The administrative state of the SAP (**Up** or **Down**).
Oper	The operational state of the SAP (**Up** or **Down**).
Stats	Whether or not statistics collection is enabled for the SAP (**Yes** or **No**).
T:P	Whether or not the 802.1p priority value of traffic mapped to this SAP is trusted. (**Y** or **N**). If this value is set to untrusted (**N**), then the traffic is marked with the specified 802.1p priority value. For example, **Y:x** indicates traffic priority is trusted; **N:3** indicates traffic priority is untrusted and should be marked with an 802.1p value of 3.
ServiceId	The ID number of the service associated with the SAP.
Isid/Vnid	An SPB service instance identifier (ISID), VXLAN network identifier (VNID), or an L2 GRE Virtual Private Network (VPN) identifier. The value of this field depends on whether an SPB service, a VXLAN service, or an L2 GRE tunnel service is associated with the SAP.
Vlan Translation	Whether or not VLAN translation is enabled for the SAP (**Yes** or **No).**
Sap Description	An optional description configured for the SAP. By default, the description is blank.

Release History

Release 7.3.1; command was introduced.
Release 7.3.2; **description** field added.
Release 7.3.4; **sap** parameter added; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service access	Configures a switch port or link aggregate as a service access port.
show service l2profile	Displays the Layer 2 profile configuration for the bridge.

MIB Objects

```
alaServiceMgrPortTable
   alaServiceMgrPortID
   alaServiceMgrPortMode
   alaServiceMgrPortPortProfileID
   alaServiceMgrPortLinkStatus
   alaServiceMgrPortSapType
   alaServiceMgrPortSapCount
   alaServiceMgrPortVlanXlation
   alaServiceMgrPortDescription
```

show service

Displays information about the services configured on the switch.

show service [spb | vxlan | l2gre | *service_id***]**

Syntax Definitions

spb	Displays only the Shortest Path Bridging (SPB) services.
vxlan	Displays only the Virtual eXtensible LAN (VXLAN) services.
l2gre	Displays only the Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services.
service_id	An existing service ID number. Displays additional details about the specified service.

Defaults

By default, a list of all services is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **spb** parameter to display additional information about SPB services.
- Use the **vxlan** parameter to display additional information about VXLAN services. This parameter is supported only on the OmniSwitch 6900-Q32, OmniSwitch 6900-X72, OmniSwitch 6900-V72, and OmniSwitch 6900-C32.
- Use the **l2gre** parameter to display additional information about L2 GRE tunnel services. This parameter is supported on the OmniSwitch 6560, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, OmniSwitch 6900-X72, and OmniSwitch 9900.
- The service ID is a unique number that identifies a specific service. Information associated with the service ID is displayed.

Examples

```
-> show service
Legend: * denotes a dynamic object
All Service Info
            Svc                    SAP   Bind
ServiceId   Type  Adm  Oper Stats Count Count Description
------------+-----+----+----+-----+-----+-----+-----------------------------------
1           VxLAN Up   Up    Y    1     3     VXLAN Svc VNID 1000
2           VxLAN Up   Up    N    1     1     VXLAN Svc VNID 2000
3           VxLAN Up   Down  Y    0     0     VXLAN Svc VNID 3000
50          L2GRE Up   Down  N    0     0     L2 GRE Tunnel
100         SPB   Up   Up    Y    2     2     SPB Svc ISID 1000
200         SPB   Down Down  N    0     0     SPB Svc ISID 2000
250         L2GRE Up   Up    Y    1     1     L2GRE Svc VPNID 251
```

```
32768*      SPB   Up   Up    Y    1     1     UNP Dynamic Svc ISID 4000
32769*      VxLAN Up   Up    Y    1     3     UNP Dynamic Svc VNID 5000
32770*      L2GRE Up   Up    Y    0     1     Dynamic Service vpnid=100 for UNP

Total Services: 9
```

output definitions

ServiceId	The service ID number.
Svc Type	The type of service (**SPB**, **VXLAN**, or **L2GRE**).
Adm	The administrative state of the service (**Up** or **Down**).
Oper	The operational state of the service (**Up** or **Down**).
Stats	Whether or not statistics collection is enabled for the service.
SAP Count	The number of Service Access Points (SAPs) associated with this service.
Bind Count	The number of Service Distribution Points (SDPs) bound to this service.
Description	An optional description configured for the service.

```
-> show service spb
Legend: * denotes a dynamic object
SPB Service Info
  SystemId : 00e0.b1e7.0188,   SrcId : 0x70188,    SystemName : TOR-1
                             SAP     Bind                    MCast
ServiceId   Adm  Oper Stats Count   Count   Isid      BVlan Mode     (T/R)
-----------+----+----+-----+-------+-------+---------+-----+--------------
100         Up   Down  Y    8       4       1000      4001  Headend  (0/0)
200         Down Down  N    0       0       1001      4001  Headend  (0/0)
32768*      Up   Up    Y    23      4       1002      4001  Headend  (0/0)

Total Services: 3
```

output definitions

SystemId	The MAC address of the switch.
SrcId	The Source ID value.
System Name	The name assigned to the switch.
ServiceId	The service ID number.
Adm	The administrative state of the service (**Up** or **Down**).
Oper	The operational state of the service (**Up** or **Down**).
Stats	Whether or not statistics collection is enabled for the service.
SAP Count	The number of Service Access Points (SAPs) associated with this SPB service.
Bind Count	The number of Service Distribution Points (SDPs) bound to this SPB service.
Isid	The service instance identifier that identifies the SPB service instance within the provider backbone bridging (PBB) network. This field is displayed only for SPB services.
BVlan	The VLAN ID number for the backbone VLAN to which the SPB service is mapped. This field is displayed only for SPB services.

output definitions

MCast Mode	The multicast replication mode (**Headend**, **Tandem**, or **Hybrid**) for the service.
T/R	The number of packets transmitted and received for this service. This field is displayed only for SPB services.

```
-> show service vxlan
Legend: * denotes a dynamic object
VxLAN Service Info
                              SAP   Bind                   MCast
ServiceId   Adm  Oper Stats Count Count Vnid               Mode
-----------+----+----+-----+-----+-----+---------------+--------------------------
1           Up   Up     Y   1     3     1000 (0.1.56)   224.2.1.1 Tandem
2           Up   Up     Y   2     1     2000 (0.7.208)      -     Headend
3           Up   Up     Y   2     1     3000 (0.11.184)     -     Headend
32769*      Up   Up     Y   1     3     5000 (0.19.136) 225.1.1.1 Tandem

Total Services: 4
```

output definitions

ServiceId	The service ID number.
Adm	The administrative state of the service (**Up** or **Down**).
Oper	The operational state of the service (**Up** or **Down**).
Stats	Whether or not statistics collection is enabled for the service.
SAP Count	The number of Service Access Points (SAPs) associated with this VXLAN service.
Bind Count	The number of Service Distribution Points (SDPs) bound to this VXLAN service.
Vnid	The VXLAN network identifier (VNID) that identifies a VXLAN segment. The decimal notation format of the VNID is also included (for example, VNID 1000 is also represented as 0.1.56).
MCast Mode	The multicast replication mode (**Headend**, **Tandem**, or **Hybrid**) for the service.

```
-> show service l2gre
Legend: * denotes a dynamic object
L2GRE Service Info
                              SAP   Bind
ServiceId   Adm  Oper Stats Count Count Vpnid
-----------+----+----+-----+-----+-----+-----------------------
50          Up   Down  N    0     0     24000
250         Up   Up    Y    1     1     251
32770*      Up   Up    Y    0     1     100

Total Services: 2
```

output definitions

ServiceId	The service ID number.
Adm	The administrative state of the service (**Up** or **Down**).
Oper	The operational state of the service (**Up** or **Down**).

output definitions

Stats	Whether or not statistics collection is enabled for the service.
SAP Count	The number of Service Access Points (SAPs) associated with this L2 GRE tunnel service.
Bind Count	The number of Service Distribution Points (SDPs) bound to this L2 GRE tunnel service.
Vpnid	A GRE tunnel Virtual Private Network (VPN) ID.

```
-> show service 100
SPB Service Detailed Info
  Service Id       : 100,                  Description      : SPB Svc ISID 1000,
  ISID             : 1000,                 BVlan            : 4001,
  Multicast-Mode   : Headend,              Tx/Rx Bits       : 0/0,
  Admin Status     : Up,                   Oper Status      : Down,
  Stats Status     : Yes,                  Vlan Translation : No,
  Service Type     : SPB,                  Allocation Type  : Static,
  MTU              : 9194,                 VPN IP-MTU       : 1500,
  SAP Count        : 8,                    SDP Bind Count   : 4,
  RemoveIngressTag : No,
  Ingress Pkts     : 0,                    Ingress Bytes    : 0,
  Egress Pkts      : 0,                    Egress Bytes     : 0,
  Mgmt Change      : 10/20/2014 10:30:44,  Status Change    : 10/19/2014 13:25:19

-> show service 1
VxLAN Service Detailed Info
  Service Id       : 1,                    Description      : VXLAN Svc VNID 1000,
  VNID             : 1000 (0.1.56),
  Multicast-Mode   : Tandem,
  Admin Status     : Up,                   Oper Status      : Up,
  Stats Status     : Yes,                  Vlan Translation : No,
  Service Type     : VxLAN,                Allocation Type  : Static,
  MTU              : 9194,                 VPN IP-MTU       : 1500,
  SAP Count        : 1,                    SDP Bind Count   : 3,
  RemoveIngressTag : No,
  Ingress Pkts     : 0,                    Ingress Bytes    : 0,
  Egress Pkts      : 0,                    Egress Bytes     : 0,
  Mgmt Change      : 10/19/2014 13:20:42,  Status Change    : 10/19/2014 13:20:42

-> show service 50
L2GRE Service Detailed Info
  Service Id       : 50,                   Description      : L2 GRE Tunnel,
  VPNID            : 24000,
  Admin Status     : Up,                   Oper Status      : Down,
  Stats Status     : No,                   Vlan Translation : No,
  Service Type     : L2GRE,                Allocation Type  : Static,
  MTU              : 9194,                 VPN IP-MTU       : 1500,
  SAP Count        : 0,                    SDP Bind Count   : 0,
  RemoveIngressTag : No,                   Port Isolation   : Enable,
  Ingress Pkts     : 0,                    Ingress Bytes    : 0,
  Egress Pkts      : 0,                    Egress Bytes     : 0,
  Mgmt Change      : 11/18/2016 10:54:54,  Status Change    : 11/14/2016 04:37:04
```

output definitions

Service Id	The service identifier.
Description	An optional description configured for the service. By default, the description is blank.
ISID	The service instance identifier (I-SID) number for the SPB service. This field is only displayed for SPB services.
BVlan	The VLAN ID number for the SPB backbone VLAN (BVLAN). This field is only displayed for SPB services.
VNID	The VXLAN network identifier for the VXLAN segment. This field is only displayed for VXLAN services.
VPNID	A GRE tunnel Virtual Private Network (VPN) ID. This field is only displayed for L2 GRE tunnel services.
Multicast-Mode	The multicast replication mode for the specified service (**tandem**, **headend**, or **hybrid**). This field is not displayed for L2 GRE tunnel services.
Tx/Rx Bits	The number of bits transmitted and received for this service. This field is only displayed for SPB services.
Admin Status	The administrative state of the service (**Up** or **Down**).
Oper Status	The operational state of the service (**Up** or **Down**).
Stats Status	Whether statistics collection is enabled for the service (**Yes** or **No**).
Vlan Translation	Whether VLAN translation is enabled for the service (**Yes** or **No).**
Service Type	The type of service (**SPB**, **VXLAN**, or **L2GRE**).
Allocation Type	Whether the service was manually or dynamically created (**Static** or **Dynamic**).
MTU	The largest frame size, in octets, that the service can handle.
SAP Count	The number of SAPs associated with this service.
SDP Bind Count	The number of SDPs bound to this service.
RemoveIngressTag	Whether the customer VLAN tag is removed before the packet is encapsulated for the service (**Yes** or **No**).
Port Isolation	The status of port isolation for an L2 GRE tunnel service. When enabled, traffic between L2 GRE tunnel SAPs is dropped. Port isolation is implicitly enabled and is not configurable in this release.
Ingress Pkts	The number of packets that have ingressed on this SAP.
Ingress Bytes	The number of bytes that have ingressed on this service.
Egress Pkts	The number of packets that have egressed on this service.
Egress Bytes	The number of bytes that have egressed on this service.
Mgmt Change	The date and time of the last configuration change for this service.
Status Change	The date and time of the last operational status change for this service.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; **vxlan** parameter added.

Release 8.4.1.R02; **l2gre** parameter added.
Release 8.6R1; “Port Isolation” field added for L2 GRE tunnel services.

Related Commands

service spb	Configures an SPB service.
service vxlan	Configures a VXLAN service.
service l2gre	Configures an L2 GRE tunnel service.
show service sdp	Displays the SDP configuration for the bridge.
show service bind-sdp	Displays the Mesh SDP bindings for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcId
   alaSvcType
   alaSvcDescription
   alaSvcMtu
   alaSvcAdminStatus
   alaSvcOperStatus
   alaSvcNumSaps
   alaSvcNumSdps
   alaSvcLastMgmtChange
   alaSvcLastStatusChange
   alaSvcAllocationType
   alaSvcStatsAdminStatus
   alaSvcIsid
   alaSvcBVlan
   alaSvcMulticastMode
   alaSvcIngressPacketCount
   alaSvcIngressByteCount
   alaSvcEgressPacketCount
   alaSvcEgressByteCount
   alaSvcSapVlanXlation
   alaSvcVnid
   alaSvcRemoveIngressTag
   alaSvcVpnId
   alaSvcPortIsolation
```

show service ports

Displays the virtual ports associated with the specified Shortest Path Bridging (SPB) service, Virtual eXtensible LAN (VXLAN) service, or Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel service.

show service {*service_id* **| isid** *instance_id* **| vnid** *vxlan_id* **| vpnid** *vpn_id***} ports**

Syntax Definitions

service_id	An existing service ID number.
instance_id	Displays the virtual ports associated with the specified SPB service instance identifier (I-SID) number. The valid range is 256–16777214.
vxlan_id	Displays the virtual ports associated with the specified VXLAN network identifier (VNID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format).
vpn_id	Displays the virtual ports associated with the specified L2 GRE tunnel Virtual Private Network (VPN) ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A Service Access Point (SAP) and a Service Distribution Point (SDP) serve as virtual ports that carry traffic for the specified SPB service, VXLAN service, or L2 GRE tunnel service.
- In addition to the virtual port configuration, this command also provides the status and additional configuration information for the SPB service, VXLAN service, or L2 GRE tunnel service.
- Displaying virtual port information for VXLAN services is supported only on the OmniSwitch 6900-Q32, OmniSwitch 6900-X72, OmniSwitch 6900-V72, and OmniSwitch 6900-C32.
- Displaying virtual port information for L2 GRE tunnel services is supported on the OmniSwitch 6560, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, OmniSwitch 6900-X72, and OmniSwitch 9900.

Examples

```
-> show service 525 ports
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB Service 525 Info
 Admin : Up,    Oper  : Up,   Stats      : N,        Mtu   : 1514, VlanXlation : N,
 ISID  : 2524,  BVlan : 4004, MCast-Mode : Headend,  Tx/Rx : 0/0,  RemoveIngTag: N

                                  Sap Trusted:Priority/         Sap Description /
Identifier        Adm  Oper Stats Sdp SystemId:BVlan   Intf     Sdp SystemName
-----------------+----+----+-----+-------------------+--------+------------------
sap:1/11:2524     Up   Up    N           Y:x           1/11        -
```

```
sap:1/12:2524     Up   Up    N           Y:x           1/12        -
sap:1/13:2524     Up   Down  N           Y:x           1/13        -
sap:1/14:2524     Up   Down  N           Y:x           1/14        -
sdp:32806:525*    Up   Up    Y    e8e7.3233.1831:4004  1/1        BRIDGE-4

Total Ports: 5

-> show service isid 1500 ports
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB Service 20 Info
 Admin : Up,    Oper  : Down, Stats      : N,        Mtu   : 9194, VlanXlation : N,
 ISID  : 1500,  BVlan : 1500, MCast-Mode : Headend,  Tx/Rx : 0/0,  RemoveIngTag: N

                                 Sap Trusted:Priority/         Sap Description /
Identifier        Adm  Oper Stats Sdp SystemId:BVlan   Intf     Sdp SystemName
-----------------+----+----+-----+-------------------+--------+-------------------
sap:1/23:0              Down Down  N           Y:x           1/23        -
sap:1/23:9.10           Down Down  N           Y:x           1/23        -

Total Ports: 2
```

output definitions

Identifier	The virtual ports (SAPs or SDPs) associated with the service.
Adm	The administrative state of the virtual port (**Up** or **Down**).
Oper	The operational state of the virtual port (**Up** or **Down**).
Stats	Whether or not statistics collection is enabled for the virtual port.
Sap Trusted : Priority	Whether or not the Service Access Point (SAP) virtual port associated with the service is trusted or assigns a priority value.
Sdp SystemId : BVlan	The system ID (base MAC) and associated BVLAN for a Service Distribution Point (SDP) virtual port associated with the service.
Intf	The bridge interface (port or link aggregate) of the virtual port (SAP or SDP) that is associated with the service.
Sap Description	The description for the SAP that is associated with the service.
Sdp Systemname	The system name for the SDP bridge that is associated with the service.

```
-> show service 1 ports
Legend: (*) dyn unicast object
VxLAN Service 1 Info
  Admin : Up,        Oper  : Up,    Stats      : Y,         VlanXlation : Y,
  VNID  : 1000 (0.1.56),           MCast-Mode : Tandem,    RemoveIngTag: N

                                Sap Trusted:Priority/
Identifier       Adm  Oper Stats Sdp FarEnd Addr       Intf     Description
----------------+----+----+-----+--------------------+--------+-------------------
sap:1/3:0        Up   Up    N           Y:x           1/20        -
sap:1/3:10       Up   Up    N           Y:x           1/20        -
sdp:32770:1*     Up   Up    Y    10.10.10.2           1/1/1    PIM Group 224.2.1.1
sdp:32771:1*     Up   Up    Y    10.10.10.3           1/1/2    PIM Group 224.2.1.1
sdp:32772:1*     Up   Up    Y    10.10.10.4           1/1/1    PIM Group 224.2.1.1

Total Ports: 5
```

```
-> show service vnid 1000 ports
Legend: (*) dyn unicast object
VxLAN Service 1 Info
  Admin : Up,        Oper  : Up,    Stats      : Y,         VlanXlation : Y,
  VNID  : 1000 (0.1.56),           MCast-Mode : Tandem,    RemoveIngTag: N

                                Sap Trusted:Priority/
Identifier       Adm  Oper Stats Sdp FarEnd/Group Addr Intf     Description
-----------------+----+----+-----+--------------------+--------+------------------
sap:1/3:0        Up   Up    N           Y:x            1/20        -
sap:1/3:10       Up   Up    N           Y:x            1/20        -
sdp:10:1         Up   Up    Y    224.2.1.1               -      PIM Group 224.2.1.1
sdp:32770:1*     Up   Up    Y    10.10.10.2             1/1/1    PIM Group 224.2.1.1
sdp:32771:1*     Up   Up    Y    10.10.10.3             1/1/2    PIM Group 224.2.1.1
sdp:32772:1*     Up   Up    Y    10.10.10.4             1/1/1    PIM Group 224.2.1.1

Total Ports: 5
```

Identifier	The virtual ports (SAPs or SDPs) associated with the service.
Adm	The administrative state of the virtual port (**Up** or **Down**).
Oper	The operational state of the virtual port (**Up** or **Down**).
Stats	Whether or not statistics collection is enabled for the virtual port.
Sap Trusted:Priority	Whether or not the Service Access Point (SAP) virtual port associated with the service is trusted or assigns a priority value.
Sdp FarEnd/Group Addr	The Loopback0 IP address or the multicast group IP address for the far-end VXLAN node associated with the service.
Intf	The bridge interface (port or link aggregate) of the virtual port (SAP or SDP) that is associated with the service.
Description	An optional description configured for the service.

```
-> show service 32770 ports
Legend: (*) dyn unicast object
L2GRE Service 32770 (Dynamic Service vpnid=123 for UNP)
  Admin : Up,        Oper  : Up,    Stats      : Y,         VlanXlation : Y,
  VPNID : 100,                    RemoveIngTag: N

                                Sap Trusted:Priority/
Identifier       Adm  Oper Stats Sdp FarEnd Addr       Intf     Description
-----------------+----+----+-----+--------------------+--------+------------------
sap:1/1/3:10     Up   Up    N           Y:x            1/1/3     L2GRE Loopback
sdp:33001:32770* Up   Up    Y        10.10.10.2        1/1/1     L2GRE VPNID 100

Total Ports: 2

-> show service vpnid 100 ports
Legend: (*) dyn unicast object
L2GRE Service 32770 (Dynamic Service vpnid=123 for UNP)
  Admin : Up,        Oper  : Up,    Stats      : Y,         VlanXlation : Y,
  VPNID : 100,                    RemoveIngTag: N

                                Sap Trusted:Priority/
Identifier       Adm  Oper Stats Sdp FarEnd Addr       Intf     Description
-----------------+----+----+-----+--------------------+--------+------------------
sap:1/1/3:10     Up   Up    N           Y:x            1/1/3     L2GRE Loopback
```

```
sdp:33001:32770* Up   Up    Y        10.10.10.2        1/1/1     L2GRE VPNID 100
sdp:33002:32771* Up   Up    Y        10.10.10.3        1/1/2     L2GRE VPNID 100

Total Ports: 3
```

Identifier	The virtual ports (SAPs or SDPs) associated with the service.
Adm	The administrative state of the virtual port (**Up** or **Down**).
Oper	The operational state of the virtual port (**Up** or **Down**).
Stats	Whether or not statistics collection is enabled for the virtual port.
Sap Trusted:Priority	Whether or not the Service Access Point (SAP) virtual port associated with the service is trusted or assigns a priority value.
Sdp FarEnd Addr	The Loopback0 IP address of the far-end Guest Tunnel access switch that is associated with the service.
Intf	The bridge interface (port or link aggregate) of the virtual port (SAP or SDP) that is associated with the service.
Description	An optional description configured for the service.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; **vnid** parameter added for VXLAN services.
Release 8.4.1.R02; **vpnid** parameter added for L2 GRE tunnel services.

Related Commands

show service	Displays the service configuration for the bridge.
show service spb sap	Displays the service access point (SAP) configuration for a specific SAP associated with the specified SPB service.

MIB Objects

N/A

show service spb sap

Displays the configuration information for the specified Service Access Point (SAP) ID associated with the specified service. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

show service spb *service_id* **sap {port** *chassis/slot/port* **| linkagg** *agg_num***} [:0 | :all | :***qtag1* **| :***outer_qtag.inner_qtag***]**

Syntax Definitions

service_id	An existing service ID number.
chassis/slot/port	The slot and port number of the Service Access Port.
agg_id	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
:qtag	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
:*outer_qtag.inner_qtag*	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A SAP is a type of virtual port that is associated with the specified service.
- A SAP determines which traffic (untagged, single-tagged, or double-tagged) is mapped to the service associated with this SAP.

Examples

```
-> show service spb 525 sap port 1/11:2524
SAP Detailed Info
  SAP Id           : 1/11:2524,           Description      : ,
  Admin Status     : Up,                  Oper Status      : Up,
  Stats Status     : No,                  Vlan Translation : No,
  Service Type     : SPB,                 Allocation Type  : Static,
  Trusted          : Yes,                 Priority         : 0,
  Ingress Pkts     : 0,                   Ingress Bytes    : 0,
  Egress Pkts      : 0,                   Egress Bytes     : 0,
  Mgmt Change      : 08/08/2014 05:41:39, Status Change    : 08/10/2014 21:14:42
```

```
-> show service spb 200 sap port 2/10:500
SAP Detailed Info
  SAP Id           : 2/10:500,             Description      : ,
  Admin Status     : Up,                   Oper Status      : Up,
  Stats Status     : No,                   Vlan Translation : No,
  Service Type     : VXLAN,                Allocation Type  : Static,
  Trusted          : Yes,                  Priority         : 0,
  Ingress Pkts     : 0,                    Ingress Bytes    : 0,
  Egress Pkts      : 0,                    Egress Bytes     : 0,
  Mgmt Change      : 08/08/2014 06:30:29,  Status Change    : 08/10/2014 22:04:12
```

output definitions

SAP Id	The access port and encapsulation associated with the service.
Description	An optional description configured for the SAP. By default, the description is blank.
Admin Status	The administrative state of the SAP (**Up** or **Down**).
Oper Status	The operational state of the SAP (**Up** or **Down**).
Stats Status	Whether statistics collection is enabled for the SAP (**Yes** or **No**).
Vlan Translation	Whether VLAN translation is enabled for the SAP (**Yes** or **No).**
Service Type	The type of service associated with this SAP (**SPB** or **VXLAN**).
Allocation Type	Whether the service was manually or dynamically created (**Static** or **Dynamic**).
Trusted	Whether the SAP is trusted (**Yes** or **No**).
Priority	The 802.1p priority assigned to traffic mapped to this SAP. Applied only when the SAP is not trusted and a priority is specified.
Ingress Pkts	The number of packets that have ingressed on this SAP.
Ingress Bytes	The number of bytes that have ingressed on this SAP.
Egress Pkts	The number of packets that have egressed on this SAP.
Egress Bytes	The number of bytes that have egressed on this SAP.
Mgmt Change	The date and time of the last configuration change for this SAP.
Status Change	The date and time of the last operational status change for this SAP.

Release History

Release 7.3.4; command was introduced.

Related Commands

show service	Displays the service configuration for the bridge.
show service ports	Displays the virtual ports (SAP and SDPs) associated with the specified SPB or VXLAN service.

MIB Objects

```
alaSapBaseInfoTable
   alaSapSvcId
   alaSapPortId
   alaSapEncapValue
   alaSapDescription
   alaSapAdminStatus
   alaSapOperStatus
   alaSapStatsAdminStatus
   alaSapType
   alaSapAllocationType
   alaSapTrusted
   alaSapPriority
   alaSapIngressPacketCount
   alaSapIngressByteCount
   alaSapEgressPacketCount
   alaSapEgressByteCount
   alaSapLastMgmtChange
   alaSapLastStatusChange
alaServiceMgrPortTable
   alaServiceMgrPortID
   alaServiceMgrPortVlanXlation
```

show service sdp

Displays the Service Distribution Point (SDP) configuration for the bridge. An SDP is a logical service entity that tunnels traffic from one switch to another switch in the network.

show service sdp [*sdp_id***]**

Syntax Definitions

sdp_id	An existing SDP ID number.

Defaults

By default, all SDPs are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *sdp_id* parameter to display information about a specific SDP.
- Manual configuration of SDPs and SDP bindings is *not* required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.
- Dynamic SDPs are not saved to the switch configuration file.
- Manual configuration of SDPs and SDP bindings is required for VXLAN services.
- The status of automatic discovery for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the **show service sdp l2gre** command for more information.
- Displaying the SDP configuration for L2 GRE services is supported on the OmniSwitch 6560, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, OmniSwitch 6900-X72, and OmniSwitch 9900.
- Displaying the SDP configuration for VXLAN services is supported only on the OmniSwitch 6900-Q32, OmniSwitch 6900-X72, OmniSwitch 6900-V72, and OmniSwitch 6900-C32.

Examples

```
-> show service sdp
Legend: * denotes a dynamic object
All SDP Info
            FarEnd/Group Ip Addr
SdpId       FarEnd SysId:BVlan    Adm  Oper SvcType
-----------+--------------------+----+----+--------
10          224.2.1.1             Up   Up   VxLAN
20          10.10.10.2            Up   Up   VxLAN
30          10.10.10.3            Up   Up   VxLAN
40          10.10.10 4            UP   UP   L2GRE
32768*      00e0.b1e4.f5eb:4000   Up   Up   SPB
```

```
32769*      00e0.b1e7.067f:4000   Up   Up   SPB
33001*      10.10.10.2            Up   Up   L2GRE

Total SDPs: 5
```

output definitions

SdpId	A unique SDP identification number, dynamically generated by ISIS-SPB or manually configured for VXLAN services or L2 GRE tunnel services.
FarEnd/Group Addr	The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses.
FarEnd SysId:BVlan	The System ID (bridge MAC address) and associated BVLAN of the far-end SPB node of the tunnel defined by this SDP.
Adm	The administrative state of the SDP (**Up** or **Down**).
Oper	The operational state of the SDP (**Up** or **Down**).
Svc Type	The type of service traffic that this SDP will tunnel (**SPB**, **VxLAN**, or **L2GRE**).

```
-> show service sdp 10
VxLAN SDP 10 Info
  SDP-Id           : 10,                   Description      : 224.2.1.1 Group,
  Service Type     : VxLAN,                FarEnd/Group     : 224.2.1.1,
  Admin Status     : Up,                   Oper Status      : Up,
  TTL              : 64 (default),
  Allocation Type  : Static,               SDP Bind Count   : 3,
  Mgmt Change      : 05/15/2014 18:38:33,  Status Change    : 05/15/2014 18:40:23

-> show service sdp 33001
L2GRE SDP 33001 Info
SDP-Id          : 33001                  Description    : L2GRE VPNID 100,
Service Type    : L2GRE,                 FarEnd/Group   : 10.10.10.2,
Admin Status    : Up,                    Oper Status    : Up,
TTL             : 64 (default),
Allocation Type : Dynamic,               SDP Bind Count : 1,
Mgmt Change     : 10/15/2016 18:38:33,   Status Change  : 10/15/2016 18:40:23
```

SDP-Id	A unique SDP identification number manually configured for VXLAN services.
Description	An optional ASCII text description for this SDP.
Service Type	The type of service traffic that this SDP will tunnel (**SPB**, **VxLAN**, or **L2GRE**).
FarEnd/Group	The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses
Admin Status	The administrative state of the SDP (**Up** or **Down**).
Oper Status	The operational state of the SDP (**Up** or **Down**).
TTL	The time-to-live (TTL) value for this SDP.

Allocation Type	Whether the SDP was statically or dynamically created. An SDP for an SPB service is generated dynamically; an SDP for a VXLAN or L2GRE tunnel service is generated statically or dynamically through the UNP feature.
SDP Bind Count	The number of services bound to this SDP.
Mgmt Change	The date and time of the last manual change to this SDP.
Status Change	The date and time of the last status change to this SDP.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN fields added.
Release 8.4.1.R02; L2 GRE fields added.

Related Commands

show service sdp spb	Displays SDP information specific to SPB services.
show service sdp vxlan	Displays SDP information specific to VXLAN services.
show service sdp l2gre	Displays SDP information specific to L2 GRE tunnel services.
show service	Displays the service configuration for the bridge.
show service bind-sdp	Displays the Mesh SDP configuration for the bridge.

MIB Objects

```
alaSdpInfoTable
   alaSdpId
   alaSdpSvcType
   alaSdpDelivery
   alaSdpFarEndIpAddress
   alaSdpDescription
   alaSdpAdminStatus
   alaSdpOperStatus
   alaSdpLastMgmtChange
   alaSdpLastStatusChange
   alaSdpNetworkPort
   alaSdpBVlan
   alaSdpSystemId
   alaSdpSystemName
   alaSdpSpSourceId
   alaSdpAllocationType
   alaSdpDynamicType
   alaSdpBindCount
   alaSdpIsid
   alaSdpMcastPortList
   alaSdpCreationOrigin
   alaSdpAdminTTL
```

show service sdp spb

Displays the Service Distribution Point (SDP) configuration for SPB services.

show service sdp spb [sysid *mac_address* **| bvlan** *bvlan_id***]]**

Syntax Definitions

mac_address	The System ID (BMAC) of the far-end SPB node of the service tunnel defined by this SDP.
bvlan_id	The VLAN ID number of an existing SPB BVLAN.

Defaults

By default, all SDPs are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **sysid** and **bvlan** parameters to display additional information about SPB SDPs.
- Manual configuration of SDPs and SDP bindings is *not* required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.
- Dynamic SDPs are not saved to the switch configuration file.

Examples

```
-> show service sdp spb
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB SDP Info
           FarEnd                                          Bind  FarEnd
SdpId      SysId:BVlan/GroupMac   SourceId Oper Intf/Isid Count SystemName/PortList
----------+---------------------+--------+----+---------+-----+------------------
32768*     00e0.b1e4.067f:4001    0x70bd3  Up   1/3       0       BRIDGE-2
32769*     00e0.b1e7.067f:4002    0x70bd3  Up   1/2       0       BRIDGE-2

Total SDPs: 2

-> show service sdp spb sysid 00.e0.b1.e4.06.7f
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB SDP Info
           FarEnd                                          Bind  FarEnd
SdpId      SysId:BVlan/GroupMac   SourceId Oper Intf/Isid Count SystemName/PortList
----------+---------------------+--------+----+---------+-----+------------------
32768*     00e0.b1e4.067f:4001    0x70bd3  Up   1/3       0       BRIDGE-2

Total SDPs: 1
```

```
-> show service sdp spb bvlan 4002
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB SDP Info
          FarEnd                                          Bind  FarEnd
SdpId     SysId:BVlan/GroupMac   SourceId Oper Intf/Isid Count SystemName/PortList
----------+--------------------+--------+----+---------+-----+------------------
32769*    00e0.b1e7.067f:4002    0x70bd3  Up   1/2       0       BRIDGE-2

Total SDPs: 1
```

output definitions

SdpId	The unique SDP identification number that is dynamically generated by ISIS-SPB.
FarEnd SysId:BVlan/ GroupMac	The System ID (BMAC) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.
SourceId	The shortest path (SP) source ID of the bridge.
Oper	The operational state of the SDP (**Up** or **Down**).
Intf/Isid	The SPB interface (network port) on which ISIS-SPB discovered the neighbor BMAC and BVLAN.
Bind Count	The number of services bound to this SDP.
FarEnd SystemName / PortList	The system name and port list of the far-end SPB node.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; **sysid** and **bvlan** parameters added.

Related Commands

show service sdp	Displays the SDP configuration for the switch.
show service sdp vxlan	Displays SDP information specific to VXLAN services.
show service sdp l2gre	Displays SDP information specific to L2 GRE tunnel services.
show service	Displays the service configuration for the bridge.
show service bind-sdp	Displays the Mesh SDP configuration for the bridge.

MIB Objects

```
alaSdpInfoTable
   alaSdpId
   alaSdpSvcType
   alaSdpDelivery
   alaSdpFarEndIpAddress
   alaSdpDescription
   alaSdpAdminStatus
   alaSdpOperStatus
   alaSdpLastMgmtChange
   alaSdpLastStatusChange
   alaSdpNetworkPort
   alaSdpBVlan
   alaSdpSystemId
   alaSdpSystemName
   alaSdpSpSourceId
   alaSdpAllocationType
   alaSdpDynamicType
   alaSdpBindCount
   alaSdpIsid
   alaSdpMcastPortList
   alaSdpCreationOrigin
   alaSdpAdminTTL
```

show service sdp vxlan

Displays the Service Distribution Point (SDP) configuration for Virtual eXtensible LAN (VXLAN) services.

show service sdp vxlan [far-end *ip_address* | **multicast-group** *mc_group_address***]]**

Syntax Definitions

ip_address	The IP address of the Loopback0 interface for the far-end VXLAN Tunnel End Point (VTEP) node. The Loopback0 address is required on every VTEP node.
mc_group_address	The multicast IP address of the group to which the service will join. *This parameter is not supported on an OmniSwitch 6900-V72 or an OmniSwitch 6900-C32*.

Defaults

By default, all SDPs are displayed.

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- Use the **far-end** and **multicast-group** parameters to display only VXLAN SDPs associated with a specific far-end IP address or a specific multicast group IP address.
- Manual configuration of SDPs and SDP bindings for VXLAN services is required.

Examples

```
-> show service sdp vxlan
Legend: (*) dyn unicast object
VxLAN SDP Info
                                                  Bind
SdpId       FarEnd/Group Addr Adm  Oper Intf      Count TTL  Description
-----------+-----------------+----+----+---------+-----+----+--------------------
10          224.2.1.1         Up   Up    -        3     64   224.2.1.1 Group
20          10.10.10.2        Up   Up   1/1/1     2     64   To NodeB
30          10.10.10.3        Up   Up   1/1/2     1     64   To NodeC

-> show service sdp vxlan multicast-group 224.2.1.1
Legend: (*) dyn unicast object
VxLAN SDP Info
                                                  Bind
SdpId       FarEnd/Group Addr Adm  Oper Intf      Count TTL  Description
-----------+-----------------+----+----+---------+-----+----+--------------------
10          224.2.1.1         Up   Up    -        3     64   224.2.1.1 Group

Total SDPs: 1
```

```
-> show service sdp vxlan far-end 10.10.10.2
Legend: (*) dyn unicast object
VxLAN SDP Info
                                                    Bind
SdpId       FarEnd/Group Addr Adm  Oper Intf        Count TTL  Description
-----------+-----------------+----+----+---------+-----+----+--------------------
20          10.10.10.2        Up   Up   1/1/1      2     64   To NodeB

Total SDPs: 1
```

SdpId	A unique SDP identification number manually configured for VXLAN services.
FarEnd/Group Addr	The IP address (Loopback0) or multicast group IP address associated with the far-end VXLAN node of this SDP.
Adm	The administrative state of the SDP (**Up** or **Down**).
Oper	The operational state of the SDP (**Up** or **Down**).
Intf	The VXLAN interface on which the VXLAN node was discovered for a unicast SDP (this field is blank for a multicast SDP).
Bind Count	The number of services bound to this SDP.
ttl	The time-to-live (TTL) value for this SDP.
Description	An optional ASCII text description for this SDP.

Release History

Release 7.3.4; command was introduced.

Related Commands

service sdp vxlan	Configures an SDP for a VXLAN service.
show service sdp	Displays the SDP configuration for the switch.
show service sdp spb	Displays SDP information specific to SPB services.
show service sdp l2gre	Displays SDP information specific to L2 GRE tunnel services.
show service	Displays the service configuration for the bridge.
show service bind-sdp	Displays the Mesh SDP configuration for the bridge.

MIB Objects

```
alaSdpInfoTable
   alaSdpId
   alaSdpSvcType
   alaSdpDelivery
   alaSdpFarEndIpAddress
   alaSdpDescription
   alaSdpAdminStatus
   alaSdpOperStatus
   alaSdpLastMgmtChange
   alaSdpLastStatusChange
   alaSdpNetworkPort
   alaSdpBVlan
   alaSdpSystemId
   alaSdpSystemName
   alaSdpSpSourceId
   alaSdpAllocationType
   alaSdpDynamicType
   alaSdpBindCount
   alaSdpIsid
   alaSdpMcastPortList
   alaSdpCreationOrigin
   alaSdpAdminTTL
```

show service sdp l2gre

Displays the Service Distribution Point (SDP) configuration for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services.

show service sdp l2gre [far-end *ip_address***]**

Syntax Definitions

ip_address	The IP address of the Loopback0 interface for the far-end L2GRE tunnel endpoint. The Loopback0 address is required on every VTEP node.

Defaults

By default, all SDPs are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- Use the **far-end** parameter to display only L2 GRE SDPs associated with a specific far-end IP address; multicast group IP addresses are not supported.
- The status of automatic SDP discovery for L2 GRE tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the **service l2gre auto-discover** command for more information.
  - If L2 GRE automatic discovery is enabled (the default), then SDPs are automatically created and bound to L2 GRE services.
  - If L2 GRE automatic discovery is disabled, then manual configuration of SDPs and SDP bindings is required for L2 GRE services.
- This command is also supported on an OmniSwitch 6560 to display dynamically configured L2 GRE service objects, such as SDPs.

Examples

```
-> show service sdp l2gre
Legend: (*) dyn unicast object
L2GRE SDP Info
                                                  Bind
SdpId    FarEnd Addr           Adm  Oper Intf     Count TTL  Description
--------+--------------------+----+----+---------+-----+----+-------------------
33001*   10.10.10.2            Up   Up   1/1/1     1     64   L2GRE VPNID 100
33002*   10.10.10.3            Up   Up   1/1/2     1     64   L2GRE VPNID 100

-> show service sdp l2gre far-end 10.10.10.2
Legend: (*) dyn unicast object
L2GRE SDP Info
                                                  Bind
SdpId    FarEnd Addr           Adm  Oper Intf     Count TTL  Description
--------+--------------------+----+----+---------+-----+----+-------------------
33001*   10.10.10.2            Up   Up   1/1/1     1     64   L2GRE VPNID 100
```

SdpId	A unique SDP identification number manually configured for L2 GRE services.
FarEnd Addr	The IP address (Loopback0 interface) associated with the far-end L2 GRE tunnel endpoint of this SDP.
Adm	The administrative state of the SDP (**Up** or **Down**).
Oper	The operational state of the SDP (**Up** or **Down**).
Intf	The interface on which the L2 GRE tunnel endpoint was discovered for a unicast SDP.
Bind Count	The number of services bound to this SDP.
ttl	The time-to-live (TTL) value for this SDP.
Description	An optional ASCII text description for this SDP.

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

service sdp l2gre	Configures an SDP for an L2 GRE tunnel service.
show service sdp	Displays the SDP configuration for the switch.
show service sdp spb	Displays SDP information specific to SPB services.
show service sdp vxlan	Displays SDP information specific to VXLAN services.
show service	Displays the service configuration for the bridge.
show service bind-sdp	Displays the Mesh SDP configuration for the bridge.

MIB Objects

```
alaSdpInfoTable
   alaSdpId
   alaSdpSvcType
   alaSdpDelivery
   alaSdpFarEndIpAddress
   alaSdpDescription
   alaSdpAdminStatus
   alaSdpOperStatus
   alaSdpLastMgmtChange
   alaSdpLastStatusChange
   alaSdpNetworkPort
   alaSdpBVlan
   alaSdpSystemId
   alaSdpSystemName
   alaSdpSpSourceId
   alaSdpAllocationType
   alaSdpDynamicType
   alaSdpBindCount
   alaSdpIsid
   alaSdpMcastPortList
   alaSdpCreationOrigin
   alaSdpAdminTTL
```

show service bind-sdp

Displays the Service Distribution Point (SDP) binding configuration for the switch.

show service bind-sdp [*sdp_id***[:***service_id***]]**

Syntax Definitions

*sdp_id***[:***service_id***]**	Displays SDP bindings with the specified SDP ID and/or service ID number.

Defaults

By default, all SDP bindings are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Manual configuration of SDPs and SDP bindings is *not* required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.
- Dynamic SDP bindings are not saved to the switch configuration file.
- Manual configuration of SDPs and SDP bindings is required for VXLAN services.
- The status of automatic SDP discovery for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the **show service bind-sdp l2gre** command for more information.
- Displaying the SDP binding configuration for VXLAN services is supported only on the OmniSwitch 6900-Q32, OmniSwitch 6900-X72, OmniSwitch 6900-V72, and OmniSwitch 6900-C32.
- Displaying the SDP binding configuration for L2 GRE services is supported on the OmniSwitch 6560, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, OmniSwitch 6900-X72, and OmniSwitch 9900.

Examples

```
-> show service bind-sdp
Legend: * denotes a dynamic object
All Bind-SDP Info
                          FarEnd/Group Addr
SvcId    Bind-Sdp         FarEnd SysId:BVlan    Oper SvcType
--------+----------------+---------------------+----+--------
1        10:1             1.1.1.6               Up   VxLAN
1        20:1             1.1.1.2               Up   VxLAN
1        30:1             1.1.1.3               Up   VxLAN
1        100:1            224.1.1.100           Up   VxLAN
2        10:2             1.1.1.6               Up   VxLAN
2        20:2             1.1.1.2               Up   VxLAN
```

```
2        30:2             1.1.1.3               Up   VxLAN
2        200:2            224.1.1.200           Up   VxLAN
3        220:3            11.2.2.1              Up   L2GRE
100      32768:100*       00e0.b1e4.f5eb:4000   Up   SPB
100      32769:100*       e8e7.3211.cdb9:4000   Up   SPB
200      32769:200*       e8e7.3211.cdb9:4000   Up   SPB
300      32769:300*       e8e7.3211.cdb9:4000   Up   SPB
32771*   33002:32771*     10.10.10.3            Down L2GRE

Total Bind-SDPs: 14
```

output definitions

SvcId	The ID number of the service that is bound to the SDP.
Bind-SDP	The unique SDP identification number that is bound to the service number.
FarEnd/Group Addr	The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses.
FarEnd SysId:BVlan	The System ID (bridge MAC address) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.
Oper	The operational state of the SDP binding (**Up** or **Down**).
Svc Type	The type of service bound to the SDP (**SPB**, **VXLAN**, or **L2GRE**).

```
-> show service bind-sdp 10
Legend: * denotes a dynamic object
VxLAN Bind-SDP Info
SvcId    Bind-Sdp         Vnid      FarEnd/Group Addr    Oper Intf     Intf Name
--------+----------------+---------+--------------------+----+--------+------------
1        10:1             100       1.1.1.6              Up     -      Intf-101
2        10:2             200       1.1.1.6              Up     -      Intf-101

Total Bind-SDPs: 2

-> show service bind-sdp 30:2
Legend: * denotes a dynamic object
VxLAN Bind-SDP Info
SvcId    Bind-Sdp         Vnid      FarEnd/Group Addr    Oper Intf     Intf Name
--------+----------------+---------+--------------------+----+--------+------------
2        30:2             200       1.1.1.3              Up     -      Intf-101

Total Bind-SDPs: 1

-> show service bind-sdp 220
Legend: * denotes a dynamic object
L2GRE Bind-SDP Info
SvcId    Bind-Sdp         Vpnid     FarEnd/Group Addr    Oper Intf     Intf Name
--------+----------------+---------+--------------------+----+--------+------------
3        220:3            300       11.2.2.1             Down   -      vlan1

Total Bind-SDPs: 1
```

```
-> show service bind-sdp 33002:32771
Legend: * denotes a dynamic object
L2GRE Bind-SDP Info

SvcId    Bind-Sdp         Vpnid     FarEnd/Group Addr    Oper Intf     Intf Name
--------+----------------+---------+--------------------+----+--------+------------
32771    33002:32771*     400       10.10.10.3           Down   -      -

Total Bind-SDPs: 1
```

output definitions

SvcId	The ID number of the service that is bound to the SDP.
Bind-SDP	The unique SDP identification number that is bound to the service number. For example, 220:3 represents SDP 220 bound to service 3.
Vnid or Vpnid	A 24-bit numerical value that identifies a VXLAN segment ID (Vnid) or an L2 GRE tunnel segment ID (Vpnid).
FarEnd/Group Addr	The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses
Oper	The operational state of the SDP binding (**Up** or **Down**).
Intf	The VXLAN or L2 GRE interface on which the SDP binding was configured.
Intf Name	The name assigned to the VXLAN or L2 GRE interface.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN fields added.
Release 8.4.1.R02; L2 GRE fields added.

Related Commands

show service bind-sdp spb	Displays SDP binding information for SPB services.
show service bind-sdp vxlan	Displays SDP binding information for VXLAN services.
show service bind-sdp l2gre	Displays SDP binding information for L2 GRE tunnel services.
show service	Displays the service configuration for the bridge.
show service sdp	Displays the SDP configuration for the bridge.

MIB Objects

```
alaSdpBindTable
   alaSdpBindId
   alaSdpBindOperStatus
   alaSdpBindNetworkPort
   alaSdpBindVirtualPort
   alaSdpBindIsid
   alaSdpBindBVlan
   alaSdpBindSystemId
   alaSdpBindSystemName
   alaSdpBindAllocationType
   alaSdpBindCreationOrigin
   alaSdpBindFarEndIpAddress
   alaSdpBindVnid
```

show service bind-sdp spb

Displays the Service Distribution Point (SDP) binding configuration for Shortest Path Bridging (SPB) services.

show service bind-sdp [spb | isid *instance_id***]**

Syntax Definitions

spb	Displays SPB SDP bindings.
instance_id	Displays SPB SDP bindings associated with the specified service instance identifier (I-SID) number. The valid range is 256–16777214.

Defaults

By default, all SDP bindings are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **spb** parameter to display information for all SPB bindings.
- Use the **isid** parameter to display information for a specific SPB service instance.
- Manual configuration of SDPs and SDP bindings is *not* required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.
- Dynamic SDP bindings are not saved to the switch configuration file.

Examples

```
-> show service bind-sdp spb
Legend: * denotes a dynamic object
SPB Bind-SDP Info
SvcId    SdpId       Isid      FarEnd SysId:BVlan   Oper Intf     FarEnd SystemName
--------+-----------+---------+--------------------+----+-------+-----------------
1        33687:1*    1000       e8e7.3233.1831:4001  Up   1/1     Bridge-4
1        37753:1*    1000       0000.bcb6.0001:4001  Up   1/1     Ix-SPB-6
1        38169:1*    1000       0000.bcb4.0001:4001  Up   1/1     Ix-SPB-4
1        38217:1*    1000       0000.beb4.0001:4001  Up   1/1     Ix-BEB-4.1.1
1        38218:1*    1000       0000.beb4.0002:4001  Up   1/1     Ix-BEB-4.1.2
1        38219:1*    1000       0000.beb4.0003:4001  Up   1/1     Ix-BEB-4.1.3
1        38220:1*    1000       0000.beb4.0004:4001  Up   1/1     Ix-BEB-4.2.1
1        38221:1*    1000       0000.beb4.0005:4001  Up   1/1     Ix-BEB-4.2.2
1        38222:1*    1000       0000.beb4.0006:4001  Up   1/1     Ix-BEB-4.2.3
1        38223:1*    1000       0000.beb4.0007:4001  Up   1/1     Ix-BEB-4.3.1

Total Bind-SDPs: 10
```

output definitions

SvcId	The ID number of the SPB service that is bound to the SDP.
SdpId	The unique SDP identification number that is dynamically generated by ISIS-SPB and bound to the service number.
Isid	The service instance identifier (I-SID) number for the SPB service.
FarEnd SysId:BVlan	The System ID (BMAC) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.
Oper	The operational state of the SDP binding (**Up** or **Down**).
Intf	The SPB interface (network port) on which ISIS-SPB discovered the neighbor BMAC and BVLAN.
FarEnd SystemName	The system name of the far-end SPB node.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; **isid** parameter added.

Related Commands

show service bind-sdp	Displays the SDP binding configuration for the switch.
show service bind-sdp vxlan	Displays SDP binding information for VXLAN services.
show service bind-sdp l2gre	Displays SDP binding information for L2 GRE tunnel services.
show service	Displays the service configuration for the bridge.
show service sdp	Displays the SDP configuration for the bridge.

MIB Objects

```
alaSdpBindTable
   alaSdpBindId
   alaSdpBindOperStatus
   alaSdpBindNetworkPort
   alaSdpBindVirtualPort
   alaSdpBindIsid
   alaSdpBindBVlan
   alaSdpBindSystemId
   alaSdpBindSystemName
   alaSdpBindAllocationType
   alaSdpBindCreationOrigin
   alaSdpBindFarEndIpAddress
   alaSdpBindVnid
```

show service bind-sdp vxlan

Displays the Service Distribution Point (SDP) binding configuration for Virtual eXtensible LAN (VXLAN) services.

show service bind-sdp [vxlan | vnid *vxlan_id***]**

Syntax Definitions

vxlan	Displays VXLAN SDP bindings.
vxlan_id	An existing VXLAN network identifier (VNID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format).

Defaults

By default, all SDP bindings are displayed.

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- Use the **vxlan** parameter to display information for all VXLAN bindings.
- Use the **vnid** parameter to display information for a specific VNID.
- Manual configuration of SDPs and SDP bindings for VXLAN services is required.

Examples

```
-> show service bind-sdp vxlan
Legend: * denotes a dynamic object
VxLAN Bind-SDP Info
SvcId    Bind-Sdp         Vnid      FarEnd/Group Addr    Oper Intf     Intf Name
--------+----------------+---------+--------------------+----+--------+------------
1        10:1             100       1.1.1.6              Up     -      Intf-101
1        20:1             100       1.1.1.2              Up     -      Intf-110
1        30:1             100       1.1.1.3              Up     -      Intf-101
1        100:1            100       224.1.1.100          Up     -
2        10:2             200       1.1.1.6              Up     -      Intf-101
2        20:2             200       1.1.1.2              Up     -      Intf-110
2        30:2             200       1.1.1.3              Up     -      Intf-101
2        200:2            200       224.1.1.200          Up     -

Total Bind-SDPs: 8
```

```
-> show service bind-sdp vnid 200
Legend: * denotes a dynamic object
VxLAN Bind-SDP Info
SvcId    Bind-Sdp         Vnid      FarEnd/Group Addr    Oper Intf     Intf Name
--------+----------------+---------+--------------------+----+--------+-----------
2        10:2             200       1.1.1.6              Up     -      Intf-101
2        20:2             200       1.1.1.2              Up     -      Intf-110
2        30:2             200       1.1.1.3              Up     -      Intf-101
2        200:2            200       224.1.1.200          Up     -

Total Bind-SDPs: 4
```

SvcId	The ID number of the service that is bound to the SDP.
Bind-SDP	The unique SDP identification number that is bound to the service number. For example, 200:2 represents SDP 200 bound to service 2.
Vnid	A 24-bit numerical value that identifies a VXLAN segment.
FarEnd/Group Addr	The IP address (Loopback0) or multicast group IP address associated with the far-end VXLAN node of the SDP.
Oper	The operational state of the SDP binding (**Up** or **Down**).
Intf	The VXLAN interface on which the SDP binding was configured.
Intf Name	The name assigned to the VXLAN interface.

Release History

Release 7.3.4; command was introduced.

Related Commands

show service bind-sdp	Displays the SDP binding configuration for the switch.
show service bind-sdp spb	Displays SDP binding information for SPB services.
show service bind-sdp l2gre	Displays SDP binding information for L2 GRE tunnel services.
show service	Displays the service configuration for the bridge.
show service sdp	Displays the SDP configuration for the bridge.

MIB Objects

```
alaSdpBindTable
   alaSdpBindId
   alaSdpBindOperStatus
   alaSdpBindNetworkPort
   alaSdpBindVirtualPort
   alaSdpBindIsid
   alaSdpBindBVlan
   alaSdpBindSystemId
   alaSdpBindSystemName
   alaSdpBindAllocationType
   alaSdpBindCreationOrigin
   alaSdpBindFarEndIpAddress
   alaSdpBindVnid
```

show service bind-sdp l2gre

Displays the Service Distribution Point (SDP) binding configuration for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services.

show service bind-sdp [l2gre | vpnid *vpn_id***]**

Syntax Definitions

l2gre	Displays L2 GRE SDP bindings.
vpn_id	An existing VPN ID for an L2 GRE tunnel segment.

Defaults

By default, all SDP bindings are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- Use the **l2gre** parameter to display information for all L2 GRE bindings.
- Use the **vpnid** parameter to display information for a specific L2 GRE VPN segment.
- The status of automatic SDP discovery for L2 GRE tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the **service l2gre auto-discover** command for more information.
  - If L2 GRE automatic discovery is enabled (the default), then SDPs are automatically created and bound to L2 GRE services.
  - If L2 GRE automatic discovery is disabled, then manual configuration of SDPs and SDP bindings is required for L2 GRE services.
- This command is also supported on an OmniSwitch 6560 to display dynamically configured L2 GRE service objects, such as SDP bindings.

Examples

```
-> show service bind-sdp l2gre
Legend: * denotes a dynamic object
L2GRE Bind-SDP Info
SvcId    Bind-Sdp         Vpnid     FarEnd/Group Addr    Oper Intf     Intf Name
--------+----------------+---------+--------------------+----+--------+------------
3        220:3            300       11.2.2.1             Down   -      vlan1
32771    33002:32771*     400       10.10.10.3           Down   -      -

Total Bind-SDPs: 2

-> show service bind-sdp vpnid 300
Legend: * denotes a dynamic object
L2GRE Bind-SDP Info
SvcId    Bind-Sdp         Vpnid     FarEnd/Group Addr    Oper Intf     Intf Name
--------+----------------+---------+--------------------+----+--------+------------
```

```
3        220:3            300       11.2.2.1            Down   -      vlan1

Total Bind-SDPs: 1
```

SvcId	The ID number of the service that is bound to the SDP.
Bind-SDP	The unique SDP identification number that is bound to the service number. For example, 220:3 represents SDP 220 bound to service 3.
Vpnid	The VPN ID for an L2 GRE tunnel segment.
FarEnd/Group Addr	The IP address (Loopback0 interface) associated with the far-end L2 GRE tunnel endpoint of the SDP.
Oper	The operational state of the SDP binding (**Up** or **Down**).
Intf	The L2 GRE interface on which the SDP binding was configured.
Intf Name	The name assigned to the L2 GRE interface.

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

show service bind-sdp	Displays the SDP binding configuration for the switch.
show service bind-sdp vxlan	Displays SDP binding information for VXLAN services.
show service bind-sdp spb	Displays SDP binding information for SPB services.
show service	Displays the service configuration for the bridge.
show service sdp	Displays the SDP configuration for the bridge.

MIB Objects

```
alaSdpBindTable
   alaSdpBindId
   alaSdpBindOperStatus
   alaSdpBindNetworkPort
   alaSdpBindVirtualPort
   alaSdpBindIsid
   alaSdpBindBVlan
   alaSdpBindSystemId
   alaSdpBindSystemName
   alaSdpBindAllocationType
   alaSdpBindCreationOrigin
   alaSdpBindFarEndIpAddress
   alaSdpBindVnid
```

show service debug-info

Displays debug information for the virtual ports associated with the service.

show service {*service_id* **| isid** *instance_id* **| vnid** *vxlan_id* **| vpnid** *vpn_id***} debug-info**

Syntax Definitions

service_id	An existing service ID number.
instance_id	Displays debug information for the SPB service associated with the specified service instance identifier (I-SID) number. The valid range is 256–16777214.
vxlan_id	Displays debug information for the VXLAN service associated with the specified VXLAN network identifier (VNID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format).
vpn_id	Displays debug information for the L2 GRE tunnel service associated with the specified Virtual Private Network (VPN) ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is associated with the specified service.
- In addition to the virtual port configuration, this command also provides the status and additional configuration information for the service.
- Use the **isid** parameter to display debug information for the SPB service associated with the I-SID.
- Use the **vnid** parameter to display debug information for the VXLAN service associated with the VNID. This parameter is supported only on the OmniSwitch 6900-Q32, OmniSwitch 6900-X72, OmniSwitch 6900-V72, and OmniSwitch 6900-C32.
- Use the **vpnid** parameter to display debug information for the L2 GRE tunnel service associated with the VPNID. This parameter is supported on the OmniSwitch 6560, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, OmniSwitch 6900-X72, and OmniSwitch 9900.

Examples

```
-> show service 20 debug-info
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB Service 20 Debug Info
 Admin : Up,   Oper  : Down, Stats      : N,       Mtu     : 9194, VlanXlation : N,
 ISID  : 1500, BVlan : 1500, MCast-Mode : Headend, Tx/Rx   : 0/0,
  VFI   : 2,   McIdx : 4094, StatsHandle: 0
```

```
                              Sap Trusted:Priority/     Sap Description/   Stats/
Identifier    Adm  Oper Stats Sdp SystemId:BVlan  Intf  Sdp SystemName VP  L2 McIdx
------------+----+----+-----+------------------+-----+--------------+---+--------
sap:1/23:0    Down Down N           Y:x           1/1/2      -         2   0
sap:1/23:9.10 Down Down N           Y:x           1/1/2      -         3   0

Total Ports: 2
-> show service 10 debug-info
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
VxLAN Service 10 Debug Info
  Admin : Up,        Oper  : Down,   Stats      : N,        VlanXlation : N,
  VNID  : 25000 (0.97.168),          MCast-Mode : Hybrid,
  VFI   : 1,         McIdx : 4095,   StatsHandle: 0

                              Sap Trusted:Priority/      Sap Description/   Stats/
Identifier   Adm  Oper Stats Sdp FarEnd/Group    Intf   Sdp Intf Name  VP  L2 McIdx
-----------+----+----+-----+------------------+------+--------------+---+--------
sap:1/22:0   Up   Down N           Y:x           1/1/22 TOR-5          1   0
sap:1/22:all Up   Down N           N:0           1/1/22    -           4   0
sap:1/22:2.5 Up   Down N           Y:x           1/1/22    -           5   0

-> show service vpnid 200 debug-info
Legend: * denotes a dynamic object
L2GRE Service 20 (Guest)
  Admin : Up,        Oper  : Up,     Stats      : N,        VlanXlation : N,
  VPNID  : 200,                     RemoveIngTag: N,
  VFI   : 2,         StatsHandle: 0

                              Sap Trusted:Priority/      Sap Description/   Stats/
Identifier   Adm  Oper Stats Sdp FarEnd/Group    Intf   Sdp Intf Name  VP  L2 McIdx
-----------+----+----+-----+------------------+------+--------------+---+--------
sap:1/1/23:0 Up   Down  N           Y:x           1/1/23 L2GRE-Loopack  3   0
sdp:200:20   Up   Up    Y    11.2.2.3               -   L2GRE-VPNID200 4   1

Total Ports: 2
```

output definitions

Identifier	The virtual ports (SAPs or SDPs) associated with the service.
Adm	The administrative state of the virtual port (**Up** or **Down**).
Oper	The operational state of the virtual port (**Up** or **Down**).
Stats	Whether statistics collection is enabled for the virtual port.
Sap Trusted : Priority	Whether the Service Access Point (SAP) virtual port associated with the service is trusted or assigns a priority value.
Sdp SystemId : BVlan	The system ID (base MAC) and associated BVLAN for a Service Distribution Point (SDP) virtual port associated with the service. This value is displayed only for SPB services.
Sdp FarEnd/Group	The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or the L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses. This value is displayed only for VXLAN and L2 GRE services.

output definitions

Intf	The switch interface (port or link aggregate) of the virtual port (SAP or SDP) that is associated with the service.
Sap Description	The description for the SAP that is associated with the service.
Sdp Systemname	The system name for the SDP bridge that is associated with the service. This value is displayed only for SPB services.
Sdp Intf Name	The name assigned to the VXLAN or L2 GRE tunnel interface. This value is displayed only for VXLAN and L2 GRE services.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; **vnid** parameter and display fields added for VXLAN.
Release 8.4.1.R02; **vpnid** parameter and display fields added for L2 GRE.

Related Commands

show service ports	Displays the virtual port (SAP and SDP) configuration for the specified service.
show service	Displays the service configuration for the bridge.
show service access	Displays the service access port configuration for the switch.

MIB Objects

N/A

show service info

Displays the Service Manager configuration for the local switch.

show service info

Syntax Definitions

N/A

Defaults

By default, the UDP port value is set to 4789.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The display output of this command also includes SPB and VXLAN information, such as the system MAC address and name used by SPB and the UDP port and VRF used by VXLAN.
- Layer 2 Generic Routing Encapsulation (L2 GRE) information is displayed based on the switch platform. For example, the status of automatic discovery and the reserved VLAN ID is displayed only on those switches that support that functionality.

Examples

Sample output on an OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900, and OmniSwitch 9900:

```
-> show service info
Service Manager System Info
  SPB System Id    : 00e0.b1e7.09a3,       SPB System Name  : OS6860,
  Service Trap     : Disable,              SAP Trap         : Disable,
  SDP Trap         : Disable,              Bind Trap        : Disable,
  Trap Rate Per Min: 60,                   VRRP TCAM Rule   : Enable,
  Stats Admin State: Enable,               Stats Owner      : SvcMgr,
  VxLAN Udp Port   : 4789,                 VxLAN Current VRF: Default,
  Mgmt Change      : 07/01/2018 11:05:04,  Status Change    : 06/24/2018 13:36:28
  SDP auto-create  : Enable
```

Sample output on an OmniSwitch 6560:

```
-> show service info
Service Manager System Info
  SPB System Id    : 2cfa.a2a2.e93f,       SPB System Name  : OS6560,
  Service Trap     : Disable,              SAP Trap         : Disable,
  SDP Trap         : Disable,              Bind Trap        : Disable,
  Trap Rate Per Min: 60,                   VRRP TCAM Rule   : Enable,
  Stats Admin State: Disable,              Stats Owner      : Available,
  VxLAN Udp Port   : 4789,                 VxLAN Current VRF: Default,
  Mgmt Change      : 07/17/2018 10:21:56,  Status Change    : 07/17/2018 10:21:56,
  L2GRE Rsvd VLAN  : 4000, 4005, 4006, 4007, 4008, 4015, 4016, 4017
```

output definitions

SPB System Id	The base MAC address of the local switch.
SPB System Name	The system name associated with the local switch.
Service Trap	The status (**Enable** or **Disable**) of trap generation for service status changes.
SAP Trap	The status (**Enable** or **Disable**) of trap generation to for SAP status changes.
SDP Trap	The status (**Enable** or **Disable**) of trap generation for SDP status changes.
Bind Trap	The status (**Enable** or **Disable**) of trap generation for service bind status changes.
Trap Rate Per Min	The maximum number of traps that can be sent per minuter.
VRRP TCAM Rule	The status (**Enable** or **Disable**) of how the switch processes VRRP packets (destination VRRP MAC address) received on access ports. When enabled, the customer VLAN tag is removed from VRRP packets. When disabled, the customer VLAN tag is *not* removed from VRRP packets. Configured through the **service local-vrrp** command.
Stats Admin State	The administrative status (**Enable** or **Disable**) of the statistics collection function. Configured through the **service stats** command.
Stats Owner	The system application in control of statistics collection.
VxLAN Udp Port	The UDP destination port for the Virtual eXtensible Local Area Network (VXLAN) feature. Configured through the **service vxlan udp-port** command.
VxLAN Current VRF	The name of the VRF instance for the VXLAN feature. Configured through the **service vxlan vrf** command.
Mgmt Change	The date and time of the last administrative status change.
Status Change	The date and time of the last operational status change.
SDP auto-create	The status (**Enable** or **Disable**) of automatic edge switch discovery on an L2 GRE tunnel aggregation switch. Configured through the **service l2gre auto-discover** command. *Supported only on the OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900, and OmniSwitch 9900.*
L2GRE Rsvd VLAN	The reserved VLAN IDs for L2 GRE tunnel services. Configured through the **service l2gre reserved-vlan** command *Supported only on the OmniSwitch 6560.*

Release History

Release 7.3.4; command was introduced; VXLAN fields added.
Release 8.3.1.R02; **VRRP TCAM Rule** field added.
Release 8.5R2; **L2GRE auto-disc** and **L2GRE Rsvd VLAN** fields added for L2 GRE tunnel services.
Release 8.5R4; **L2GRE auto-disc** field name changed to **SDP auto-create**.
Release 8.6R1; **L2GRE Rsvd VLAN** field allows display of multiple L2 GRE reserved VLANs.

Related Commands

show service	Displays information about the services configured on the switch.

MIB Objects

```
alaSvcMgrSysTable
   alaSvcMgrSysId
   alaSvcMgrSysName
   alaSvcMgrSysLastMgmtChang
   alaSvcMgrSysLastStatusChange
   alaSvcMgrSvcTrapAdminState
   alaSvcMgrSapTrapAdminState
   alaSvcMgrSdpTrapAdminState
   alaSvcMgrSdpBindTrapAdminStat
   alaSvcMgrMaxTrapPerMinute
   alaSvcMgrVrrpMacTcamRuleAdminState
   alaSvcMgrVxlanDestUdpPort
   alaSvcMgrVxlanVrfName
   alaSvcMgrSdpAutoCreateAdminState
   alaSvcMgrReservedL2greVlan
```

show service counters

Displays the traffic statistics for the specified service and associated virtual ports. A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is bound to the specified service.

show service {*service_id* **| vnid** *vxlan_id* **| vpnid** *vpn_id***} counters**

Syntax Definitions

service_id	An existing service ID number.
vxlan_id	Displays statistics for the VXLAN service associated with the specified VXLAN network identifier (VNID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format).
vpn_id	Displays statistics for the L2 GRE tunnel service associated with the specified Virtual Private Network (VPN) ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Enter an existing service ID number to display statistics for a specific service.
- Use the **vnid** parameter to display statistics for a specific VXLAN network identifier. A VNID identifies a specific VXLAN network segment. This parameter is supported only on the OmniSwitch 6900-Q32 and OmniSwitch 6900-X72.
- Use the **vpnid** parameter to display statistics for a specific L2 GRE VPN segment. This parameter is supported only on the OmniSwitch 6560, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, and OmniSwitch 6900-X72.

Examples

```
-> show service 20 counters
Legend: * denotes a dynamic object

Identifier              Ing Pkts   Ing Byte Count  Egr Pkts   Egr Byte Count
----------------------+----------+---------------+----------+---------------
sap:1/1:10                1234         12345678         12            123
sap:1/1:15                1234         12345678         12            123
sap:8/2                   1234         12345678         12            123
sap:2/3:20.25*            1234         12345678         12            123
sdp:32768:100               34             5678       4321       12345678
```

```
-> show service vnid 1000 counters
Legend: * denotes a dynamic object

Identifier              Ing Pkts   Ing Byte Count  Egr Pkts   Egr Byte Count
----------------------+----------+---------------+----------+---------------
sap:1/5:20                1200         12345678         12            123
sap:2/10:30.35*           1200         12345678         12            123
sdp:32769:200               60             5678       4321       12345678

-> show service vpnid 200 counters
Legend: * denotes a dynamic object

Identifier              Ing Pkts   Ing Byte Count  Egr Pkts   Egr Byte Count
----------------------+----------+---------------+----------+---------------
sap:1/1/23:10             1200         12345678         12            123
sap:1/1/24:0              1200         12345678         12            123
sdp:200:20                  60             5678       4321       12345678
```

output definitions

Identifier	The virtual ports (SAPs or SDPs) associated with the service.
Ing Pkts	The number of packets received on the virtual port.
Ing Byte Count	The ingress packet byte count for the virtual port.
Egr Pkts	The number of packets sent on the virtual port.
Egr Byte Count	The egress packet byte count for the virtual port.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; **vnid** parameter added for VXLAN.
Release 8.4.1.R02; **vpnid** parameter added for L2 GRE.

Related Commands

show service	Displays the service configuration for the bridge.
show service ports	Displays the virtual ports associated with the specified service.
clear service counters	Clears the traffic statistics for the specified service and associated virtual ports.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcIngressPacketCount
   alaSvcIngressByteCount
   alaSvcEgressPacketCount
   alaSvcEgressByteCount
```

clear service counters

Clears the traffic statistics for the specified service and associated virtual ports. A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is bound to the specified service.

clear service [*service_id***] [sap {port** *chassis/slot/port* | **linkagg** *agg_id***}[:0 | :all | :***qtag* **| :***outer_qtag.inner_qtag***] | mesh-sdp** *sdp_id***] counters**

Syntax Definitions

service_id	An existing SPB service ID number.
chassis	The chassis identifier.
slot/port	The slot and port number of the service access port.
agg_id	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wild-card SAP. All tagged traffic that is not classified into another SAP is mapped to the wild-card SAP.
:qtag	Specifies a VLAN ID tag for traffic that ingresses on the access port. Only traffic with this tag is mapped to this SAP.
:*outer_qtag.inner_qtag*	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic that ingresses on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
sdp_id	An existing mesh SDP ID.

Defaults

By default, all statistics counters for the specified service are cleared.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **sap** parameter options with this command to clear the statistics for a specific SAP ID. A SAP ID is comprised of an access port (*slot*/*port* or *agg_id*) and an encapsulation value (**:0**, **:all**, **:***qtag*, or **:***outer_qtag.inner_qtag*) that is used to identify the type of customer traffic to map to the associated service.
- Use the **mesh-sdp** *sdp_id* parameter to clear the statistics for a specific mesh SDP.

Examples

```
-> clear service counters
-> clear service 100 counters
-> clear service sap 8/2:all counters
-> clear service mesh-sdp counters
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.

Related Commands

show service counters	Displays the traffic statistics for the specified SPB service and associated virtual ports.

MIB Objects

```
alaSvcBaseInfoTable
   alaSvcClearCounters
alaSapBaseInfoTable
   alaSapClearCounters
```

show service rfp

Displays the configuration and status of SPB Remote Fault Propagation (RFP) domains.

show service rfp [*rfp_id* **[local-sap-status]]**

Syntax Definitions

rfp_id	An existing RFP ID number.
local-sap-status	Displays information about the local SPB service elements that are bound to the specified RFP ID.

Defaults

By default, information for all RFP domains is displayed.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Enter an existing RFP ID number to display statistics for a specific RFP domain.
- Use the **local-sap-status** parameter to display SPB service information for the specified RFP ID.

Examples

```
-> show service rfp

Local system (Name: SystemId) = bridge1 : E8:E7:32:B8:9C:98
Total number of services information =6
Total Number of RFP domain           =2
RFP  Remote   RMEP     System                    B-VLAN   ISID   Service  Admin
     EndPoint Status  (Name: SystemId)                          Id       State
----+--------+--------+-------------------------+------+--------+--------+---------
1000     2    RMEP_OK  bridge2:E8:E7:32:B8:9C:95  4001   10000     10     Enable
1000     3    RMEP_OK  bridge3:E8:E7:32:B8:9C:90  4002   20000     20     Enable
1000     4    RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4003   30000     30     Enable
2000     4    RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4004   40000     40     Enable
2000     4    RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4005   50000     50     Enable
2000     4    RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4006   60000     60     Enable

-> show service rfp 1000

Local system (Name: SystemId) = bridge1 : E8:E7:32:B8:9C:98
Total number of services information =6
Total Number of RFP domain           =2
RFP  Remote   RMEP     System                    B-VLAN   ISID   Service  Admin
     EndPoint Status  (Name: SystemId)                          Id       State
----+--------+--------+-------------------------+------+--------+--------+---------
1000     2    RMEP_OK  bridge2:E8:E7:32:B8:9C:95  4001   10000     10     Enable
1000     3    RMEP_OK  bridge3:E8:E7:32:B8:9C:90  4002   20000     20     Enable
1000     4    RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4003   30000     30     Enable
```

output definitions

RFP	The RFP ID number. Configured through the **service rfp local-endpoint** command.
Remote EndPoint	The ID number for the RFP remote end point. Configured through the **service rfp remote-endpoint** command.
RMEP Status	The status of the remote Maintenance End Point (MEP).
System (Name: SystemId)	The name and bridge MAC address of the remote SPB switch.
B-VLAN	The SPB backbone VLAN that serves as the primary VLAN for the RFP domain. The SPB control BVLAN is automatically used for each RFP OAM domain.
ISID	The SPB service instance ID. The ISID is bound to an SPB service ID, which in turn is bound to an SPB access port. This binding creates a Service Access Point (SAP), which is configured through the **service sap** command.
Service Id	An SPB service ID number. Configured through the **service spb** command and associated with the RFP ID through the **service rfp remote-endpoint** command.
Admin State	The administrative status (**Enable** or **Disable**) of the SAP port on the local chassis.

```
-> show service rfp 1000 local-sap-status

Local endpoint ID = 10
Local system (Name: SystemId) = bridge1 : E8:E7:32:B8:9C:98

Service Sap             Admin   Oper     Remote   R-Endpoint
Id                                       EndPoint Status
-------+---------------+-------+-------+--------+-----------+
10      sap:1/11:10     Enable  Up        2        RMEP_OK
20      sap:1/10:10     Enable  Up        3        RMEP_OK
30      sap:2/11:10     Enable  Violation 4        RMEP_FAILED
40      sap:2/12:10     Enable  Down      4        RMEP_FAILED
50      sap:2/13:10     Enable  Down      4        RMEP_FAILED
```

Local endpoint ID	The ID number of the local RFP end point.
Local system (Name: SystemId)	The name and bridge MAC address of the local SPB switch.
Service Id	An SPB service ID number. Configured through the **service spb** command and associated with the RFP ID through the **service rfp remote-endpoint** command.
Sap	The Service Access Point to which the SPB service ID is associated through the configured through the **service sap** command
Admin State	The administrative status (**Enable** or **Disable**) of the SAP.
Oper	The operation status (**Up**, **Down**, **Violation**) of the SAP.
Remote EndPoint	The ID number for the RFP remote end point. Configured through the **service rfp remote-endpoint** command.
R-Endpoint Status	The status of the remote Maintenance End Point (MEP).

Release History

Release 7.3.4; command was introduced.

Related Commands

show service rfp configuration Displays the RFP OAM domain configuration for the bridge.

MIB Objects

N/A

show service rfp configuration

Displays the RFP OAM domain configuration for the bridge. When an RFP domain is created, an Ethernet OAM domain is automatically configured on the switch and mapped to the RFP domain.

show service rfp configuration [*rfp_id***]**

Syntax Definitions

rfp_id	An existing RFP ID number.

Defaults

By default, information for all RFP OAM domains is displayed.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Enter an existing RFP ID number to display the OAM domain configuration for a specific RFM domain.
- For each RFP domain created, a separate OAM domain is also created and mapped to the RFP domain.

Examples

```
-> show service rfp configuration
Total Number of RFP domains - 2

RFP domain Number      : 1000
Admin status           : Enabled
Level                  : 7
Type                   : SPB
Maintenance Domain     : RFP_OVER_SPB_DOMAIN_LEVEL7
Maintenance Association: RFP_OVER_SPB_ASSOCIATION
Control B-VLAN         : 1000
Virtual UP MEP ID      : 10
CCM interval           : 100 millisecond
Remote Endpoint service ID
---------------+----------
1               10,11
2               20
3-9             40

RFP domain Number      : 2000
Admin status           : Enabled
Level                  : 6
Type                   : SPB
Maintenance Domain     : RFP_OVER_SPB_DOMAIN_LEVEL6
Maintenance Association: RFP_OVER_SPB_ASSOCIATION
Control B-VLAN         : 1000
Virtual UP MEP ID      : 10
CCM interval           : 100 millisecond
```

```
Remote Endpoint service ID
---------------+----------
1                30,31
2                50
3-9              70

-> show service rfp configuration 1000

RFP domain Number      : 1000
Admin status           : Enabled
Level                  : 7
Type                   : SPB
Maintenance Domain     : RFP_OVER_SPB_DOMAIN_LEVEL7
Maintenance Association: RFP_OVER_SPB_ASSOCIATION
Control B-VLAN         : 1000
Virtual UP MEP ID      : 10
CCM interval           : 100 millisecond
Remote Endpoint service ID
---------------+----------
1                10,11
2                20
3-9              40
```

output definitions

RFP domain number	The RFP ID number. that is mapped to the OAM domain.
Admin State	The administrative status (**Enable** or **Disable**) of the RFP domain.
Level	The Maintenance Domain (MD) level.
Type	The type of RFP domain (SPB is the only type currently supported).
Maintenance Domain	The name of the reserved MD assigned to the RFP domain.
Maintenance Association	The name of the Maintenance Association (MA) for the RFP (MD). The same MA name is used for all RFP domains.
Control B-VLAN	The SPB control BVLAN that serves as the primary VLAN for the RFP OAM domain.
Virtual UP MEP ID	The local end point ID for the RFP domain.
CCM interval	The time interval at which a Continuity Check Message (CCM) is sent for this domain.
Remote Endpoint	The RFP ID number for the remote end point.
service ID	The SPB service ID number associated with the remote end point ID.

Release History

Release 7.3.4; command was introduced.

Related Commands

show service rfp	Displays the configuration and status of SPB Remote Fault Propagation (RFP) domains.

MIB Objects

N/A

11 Loopback Detection Commands

Loopback Detection (LBD) automatically detects the loop and shutdown the port involved in the loop. This prevents forwarding loops on ports that have forwarded network traffic which has looped back to the originating switch. LBD detects and prevents Layer 2 forwarding loops on a port either in the absence of other loop detection mechanisms such as STP/RSTP/MSTP, or when these mechanisms cannot detect it (for example, a client's equipment may drop BPDUs, or the STP protocol may be restricted to the network edge). On a linkagg port, if one port of linkagg is getting shutdown due to LBD, then all the ports of linkagg will go to shutdown state.

Loopback Detection is enabled system wide and on a per-port basis. Once a loop is discovered, the port from which the loop originated is placed into an “Inactive” state and when the two ports of a switch is connected to each other through a hub, either the ports will be shutdown or it will be in normal state.

A provider network with a set of multiple switches interconnected together can be logically viewed as a large single switch. The large single switch provides service access points to customers' networks. Configuration faults in customer networks can result in loops spanning both provider and customer networks. This can result in broadcast storms. In order to protect provider's network from broadcast storms, loops that involve SAP ports need to be detected and broken.

The LBD can detect and break loops created on the service-access interface.

For a service-access interface, LBD can be enabled for a specific port or linkagg. LBD for service-access points allows shutting down only the specific interface of the link involved in the loop.

When loopback occurs, a trap is sent and the event is logged. The port which is shutdown due to LBD is automatically recovered if autorecovery-timer is set or the port can manually be enabled again when the problem is resolved.

MIB information for the Loopback Detection commands is as follows:

Filename: ALCATEL-IND1-LBD-MIB
Module: alcatelIND1LBDMIB

A summary of available commands is listed here:

loopback-detection

Enables or disables Loopback Detection (LBD) or remote origin LBD globally on the switch.

loopback-detection [remote-origin] {enable | disable}

Syntax Definitions

enable	Enables LBD on the switch.
disable	Disables LBD on the switch.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- LBD can be enabled globally and per port without any dependency but loopback-detection will be operational only if LBD is enabled globally and also on the specific port.
- LBD can be configured for a port and the configuration can be applied and retained, whether or not LBD is enabled globally. However, LBD functionality on a port is available only when LBD is enabled globally on the switch.
- Enabling the **remote-origin** LBD option allows the switch to process the LBD frames originated from a remote system. The port from which the LBD frames originated will be shut down.

Examples

```
-> loopback-detection enable
-> loopback-detection disable
-> loopback-detection remote-origin enable
-> loopback-detection remote-origin disable
```

Release History

Release 7.3.4; command was introduced.
Release 8.2.1; **remote-origin** parameter added.

Related Commands

loopback-detection port	Enables or disables LBD on a specific port.
show loopback-detection	Displays LBD configuration information.

MIB Objects

```
alaLbdGlobalConfigStatus
alaLbdGlobalRemoteConfigStatus
```

loopback-detection port

Enables or disables LBD or remote-origin LBD on a specific bridge port.

loopback-detection port *chassis/slot/port***[-***port2***] [remote-origin] {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
enable	Enables LBD on the specified port.
disable	Disables LBD on the specified port.

Defaults

parameter	default
enable | **disable**	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Loopback Detection must be enabled globally to enable LBD functionality on a specific port.
- For per-port remote origin LBD to work, both LBD and remote origin LBD must be enabled globally.
- LBD can be configured for a port and the configuration can be applied and retained, whether or not LBD is enabled globally. However, LBD functionality on a port is available only when LBD is enabled globally on the switch.
- When a LBD port joins a link aggregate, the LBD configuration on the joined port is removed.

Examples

```
-> loopback-detection port 1/1/1 enable
-> loopback-detection port 1/1/1-8 enable
-> loopback-detection port 1/1/2 remote-origin enable
-> loopback-detection port 1/1/3-5 remote-origin enable
-> loopback-detection port 1/1/2 remote-origin disable
-> loopback-detection port 1/1/3-5 remote-origin disable
```

Release History

Release 7.3.4; command was introduced.
Release 8.2.1; **remote-origin** parameter added.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information.
show loopback-detection port	Displays LBD port configuration information.

MIB Objects

```
alaLbdPortConfigTable
   alaLbdPortConfigEntry
   alaLbdPortConfigIndex
   alaLbdPortConfigLbdAdminStatus
   alaLbdPortConfigLbdOperStatus
   alaLbdPortRemoteConfigAdminStatus
```

loopback-detection service-access

Enables or disables LBD on a specific service access port or link aggregate or on a range of ports or link aggregates. When enabled, LBD can detect and break loops created on a service access interface.

loopback-detection service-access {port *chassis/slot/port*[*-port2*] | **linkagg** *agg_id***[-***agg_id2***]} {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables LBD on the specified port or linkagg.
disable	Disables LBD on the specified port or linkagg.

Defaults

parameter	default
enable | **disable**	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Before configuring LBD using the **service-access** option, the port or linkagg must be configured for service access. Use the **service access** command to configure the port or linkagg for service access.
- The **service-access** option allows shutting down only the specific interface of the link involved in the loop.
- The linkagg must be formed by ports with same path cost.
- LBD is applicable on a linkagg only if the linkagg is configured as a service access interface.
- LBD cannot be configured on a linkagg that has member ports running LBD configuration and vice versa.
- When a linkagg is in violation or shutdown state, the member ports cannot be deleted from the linkagg.

Examples

```
-> loopback-detection service-access port 1/1/1 enable
-> loopback-detection service-access port 1/1/1-8 enable
-> loopback-detection service-access linkagg 1 enable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information.
show loopback-detection port	Displays LBD port configuration information.
show loopback-detection linkagg	Displays LBD configuration information for a service access link aggregate.

MIB Objects

```
alaLdbPortConfigTable
   alaLdbPortConfigLdbAdminStatus
   alaLbdUserPortConfigLbdInterfaceType
```

loopback-detection transmission-timer

Configures the LBD transmission timer on the switch.The transmission time is the time period between the consecutive LBD packet transmissions.

loopback-detection transmission-timer *seconds*

Syntax Definitions

seconds	The time period in seconds between LBD packet transmissions. The valid range is from 5 to 600 seconds.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the timer value is not configured, the default value of 30 seconds is assigned to the transmission period.
- The timer can be modified at any time. However, the new timer value will come into effect only after the timer is restarted.

Examples

```
-> loopback-detection transmission-timer 200
```

Release History

Release 7.3.4; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information.

MIB Objects

```
alaLbdGLobalConfigTransmissionTimer
```

loopback-detection autorecovery-timer

Configures the LBD autorecovery timer on the switch.The autorecovery time is the time period in which the switch is recovered from the shutdown state.

loopback-detection autorecovery-timer *seconds*

Syntax Definitions

seconds	The time period in seconds in which the switch is recovered from the shutdown state. The valid range is from 30 to 86400 seconds.

Defaults

parameter	default
seconds	300

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the timer value is not configured, the default value of 300 seconds is assigned to the autorecovery period.
- The timer can be modified at any time. However, the new timer value will come into effect only after the timer is restarted.

Examples

```
-> loopback-detection autorecovery-timer 200
```

Release History

Release 7.3.4; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information.

MIB Objects

```
alaLbdGlobalConfigAutorecoveryTimer
```

show loopback-detection

Displays the global LBD configuration information for the switch.

show loopback-detection

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To view information for a specific port or service access link aggregate, use the **show loopback-detection port** or **show loopback-detection linkagg** command.

Examples

```
-> show loopback-detection
Global LBD Status                : enabled,
Global Remote-origin LBD Status  : disabled,
Global LBD Transmission Timer    : 30 sec,
Global LBD Auto-recovery Timer   : 300 sec,
```

output definitions

Global LBD Status	The current status of LBD of the switch (**enabled** or **disabled**).
Global Remote-origin LBD Status	The current status of remote-origin LBD of the switch (**enabled** or **disabled**).
Global LBD Transmission Timer	Displays the time interval in seconds between LBD packet transmissions.
Global LBD Auto-recovery Timer	Displays the time in which the switch recovered from the shutdown state.

Release History

Release 7.3.4; command was introduced.
Release 8.2.1; “Global Remote-origin LBD Status” field added.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection port	Displays LBD configuration information for bridge and service access ports on the switch.
show loopback-detection linkagg	Displays LBD configuration information for a service access link aggregate.
show violation	Displays the administrative status, link status, violations, recovery time, maximum recovery attempts and the value of the wait-to-restore timer for the specified port or ports.

MIB Objects

```
alaLbdGlobalConfigStatus
alaLbdGlobalRemoteConfigStatus
alaLbdGlobalConfigTransmissionTimer
alaLbdGlobalConfigAutorecoveryTimer
```

show loopback-detection port

Displays the LBD configuration information for the specified bridge or service access port.

show loopback-detection port [*chassis*/*slot/port*]

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1).

Defaults

By default, the LBD configuration for all ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The command can be used only on an LBD enabled port.

- Use the **loopback-detection port** command to enable LBD on a bridge port.
- Use the **loopback-detection service-access** command to enable LBD on a service access port or link aggregate.

Examples

```
-> show loopback-detection port
Slot/Port   Admin State Remote-origin Status OperState       Time-to-recovery (sec)
-----------+-----------+--------------------+---------------+----------------------
1/1/1       enabled     enabled              Remote ShutDown   -
1/1/2       enabled      -                   Normal            -
```

output definitions

Slot/Port	The slot/port number of the LBD port.
Admin State	The administrative state of the port (**enabled** or **disabled**).
Remote-origin Status	The remote-origin LBD status of the port (**enabled** or **disabled**). This field does not apply to LBD service access ports.
OperState	The operational state of the port (**Normal** or **Inactive**).
Time-to-recovery (sec)	The amount of time to recovery during an LBD shutdown.

```
-> show loopback-detection port 1/1/1
Global LBD Status                  : enabled,
Global Remote-origin LBD Status    : enabled,
Global LBD Transmission Timer      : 30 sec,
Global LBD Auto-recovery Timer     : 300 sec,
Port LBD Status                    : enabled,
Port Remote-origin LBD Status      : enabled,
```

```
Port LBD State                    : Remote ShutDown,
Remote Src Mac                    : E8:E7:32:9A:5A:4E,
Remote BridgeId                   : E8:E7:32:9A:5A:3F,
Port LBD Type                     : normal-edge,

-> show loopback-detection port 1/1/2
Global LBD Status                 : enabled,
Global Remote-origin LBD Status   : disabled,
Global LBD Transmission Timer     : 30 sec,
Global LBD Auto-recovery Timer    : 300 sec,
Port LBD Status                   : enabled,
Port Remote-origin LBD Status     : -,
Port LBD State                    : Inactive,
Port LBD Type                     : service-edge,
```

output definitions

Global LBD Status	The current status of LBD of the switch (**enabled** or **disabled**).
Global Remote-origin LBD Status	The current status of remote-origin LBD on the switch (**enabled** or **disabled**).
Global LBD Transmission Timer	Displays the time interval in seconds between LBD packet transmissions.
Global LBD Auto-recovery Timer	Displays the time interval in seconds in which the switch is recovered from the shut down state.
Port LBD Status	Displays the administrative status of the port.
Port Remote-origin LBD Status	Displays the remote-origin LBD status of the port (**enabled** or **disabled**). This field does not apply to LBD service access ports.
Port LBD State	Displays the current operational state of the port.
Remote Src Mac	Displays the MAC address of the remote system. The Remote Src Mac is displayed only if remote-origin LBD is enabled on the system.
Remote BridgeId	Displays the bridge ID of the remote system. The Remote BridgeId is displayed only if remote-origin LBD is enabled on the system.
Port LBD Type	Displays the type of the interface—whether a normal edge interface or a service access interface.

Release History

Release 7.3.4; command was introduced.
Release 8.2.1; fields added to display LBD remote origin information.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
loopback-detection port	Enables or disables LBD for a bridge port
loopback-detection service-access	Enables or disables LBD for a service access port or link aggregate.
show loopback-detection linkagg	Displays LBD configuration information for a service access link aggregate.
show loopback-detection statistics port	Displays LBD statistics information for a specific port.

MIB Objects

```
   alaLbdGlobalConfigStatus
   alaLbdGlobalRemoteConfigStatus
   alaLbdGlobalConfigTransmissionTimer
   alaLbdGlobalConfigAutorecoveryTimer
alaLbdPortConfigTable
   alaLbdPortConfigLbdAdminStatus
   alaLbdPortConfigLbdOperStatus
   alaLbdPortConfigServiceAccessType
   alaLbdPortRemoteConfigAdminStatus
   alaLbdPortRemoteSrcMacAddr
   alaLbdPortRemoteBridgeID
   alaLbdPortTimeToRecovery
```

show loopback-detection linkagg

Displays the LBD configuration information for the specified link aggregate ID.

show loopback-detection linkagg *agg_id*

Syntax Definitions

agg_id	The link aggregate ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The command can be used only on an LBD enabled link aggregate. Use the **loopback-detection service-access** command to enable LBD on a service access link aggregate.

Examples

```
-> show loopback-detection linkagg 10
Global LBD Status                    : enabled,
Global Remote-origin LBD Status      : disabled,
Global LBD Transmission Timer        : 30 sec,
Global LBD Auto-recovery Timer       : 300 sec,
Linkagg LBD Status                   : disabled,
Linkagg LBD State                    : Inactive,
Linkagg LBD Type                     : service-access
```

output definitions

Global LBD Status	The current LBD status for the switch (**enabled** or **disabled**).
Global Remote-origin LBD Status	The current status of remote-origin LBD on the switch (**enabled** or **disabled**). This field does not apply to LBD link aggregates.
Global LBD Transmission Timer	Displays the time interval in seconds between LBD packet transmissions.
Global LBD Auto-recovery Timer	Displays the time interval in seconds in which the switch is recovered from the shut down state.
Linkagg LBD Status	Displays the administrative status of the link aggregate.
Linkagg LBD State	Displays the current operational state of the link aggregate.
Linkagg LBD Type	Displays the type of the interface—whether a normal edge interface or a service access interface. LBD supported on service access link aggregates.

Release History

Release 7.3.4; command was introduced.
Release 8.2.1; fields added to display LBD remote origin information.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
loopback-detection service-access	Enables or disables LBD for a service access port or link aggregate.
show loopback-detection statistics port	Displays LBD statistics information for a specific port.

MIB Objects

```
   alaLbdGlobalConfigStatus
   alaLbdGlobalRemoteConfigStatus
   alaLbdGlobalConfigTransmissionTimer
   alaLbdGlobalConfigAutorecoveryTimer
alaLbdPortConfigTable
   alaLbdPortConfigLbdAdminStatus
   alaLbdPortConfigLbdOperStatus
   alaLbdPortConfigServiceAccessType
```

show loopback-detection statistics port

Displays LBD statistics information for a specific port on the switch.

show loopback-detection statistics port *chassis*/*slot/port*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The link aggregate ID is not displayed if the link aggregate is operationally down.

Examples

```
-> show loopback-detection statistics port 1/1/1
LBD Port Statistics
LBD Packet Send               : 1,
Invalid LBD Packet Received   : 0,
Member of Link Aggregation    : -

-> show loopback-detection statistics port 1/1/3
LBD Port Statistics
LBD Packet Send                : 1,
Invalid LBD Packet Received    : 0,
Member of Aggregation          : 2
```

output definitions

LBD Packet Send	The number of LBD packet sent from the port.
Invalid LBD Packet Received	The number of invalid LBD packets received on the port.
Member of Aggregation	The linkagg ID in which the port is a member.

Release History

Release 7.3.4; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection port	Displays LBD configuration information for a specific port.

MIB Objects

```
alaLbdPortStatsTable
   alaLbdPortStatsIfIndex
   alaLbdPortNumLbdInvalidRcvd
   alaLbdPortLbdSent
   alaLbdPortLinkAgg
```

clear loopback-detection statistics port

Clears statistics of all LBD ports or a specific port.

clear loopback-detection statistics port [*chassis*/*slot/port*]

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A.

Examples

```
-> clear loopback-detection statistics port 1/1/2
```

Release History

Release 7.3.4; command was introduced.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection port	Displays LBD configuration information for a specific port.

MIB Objects

```
alaLbdPortStatsTable
   alaLbdPortStatsClear
```

12 Link Aggregation Commands

Link aggregation combines multiple physical links between two switches into one logical link. The aggregate group operates within Spanning Tree as one virtual port and can provide more bandwidth than a single link. It also provides redundancy. If one physical link in the aggregate group goes down, link integrity is maintained.

There are two types of aggregate groups: static and dynamic. Static aggregate groups are manually configured on the switch with static links. Dynamic groups are set up on the switch but they aggregate links as necessary according to the Link Aggregation Control Protocol (LACP).

The dynamic aggregation software is compatible only with the following IEEE standard:

802.3ad — Aggregation of Multiple Link Segments

MIB information for the link aggregation commands is as follows:

Filename: ALCATEL-IND1-LAG-MIB.mib
Module: alcatelIND1LAGMIB

A summary of available commands is listed here:

Static link aggregates	**linkagg static agg size** **linkagg static agg name** **linkagg static agg wait-to-restore-time** **linkagg static agg loopback** **linkagg static agg loopback internal** **linkagg static agg admin-state** **linkagg static port agg**
Dynamic link aggregates	**linkagg lacp agg size** **linkagg lacp agg name** **linkagg lacp agg wait-to-restore-time** **linkagg lacp agg admin-state** **linkagg lacp agg actor admin-key** **linkagg lacp agg actor system-priority** **linkagg lacp agg actor system-id** **linkagg lacp agg partner system-id** **linkagg lacp agg partner system-priority** **linkagg lacp agg partner admin-key** **linkagg lacp port actor admin-key** **linkagg lacp port actor admin-state** **linkagg lacp port actor system-id** **linkagg lacp port actor system-priority** **linkagg lacp agg partner admin-state** **linkagg lacp port partner admin system-id** **linkagg lacp port partner admin-key** **linkagg lacp port partner admin system-priority** **linkagg lacp port actor port priority** **linkagg lacp port partner admin-port** **linkagg lacp port partner admin port-priority**
Dual Home Link (DHL) Active-Active	**dhl name** **dhl linka linkb** **dhl admin-state** **dhl vlan-map linkb** **dhl pre-emption-time** **dhl mac-flushing** **show dhl** **show dhl link**
Static and dynamic	**linkagg range** **show linkagg range** **show linkagg** **show linkagg port** **show linkagg accounting** **show linkagg counters** **show linkagg traffic** **clear linkagg-statistics**

linkagg static agg size

Creates a static aggregate group between two switches. A static aggregate group contains static links.

linkagg static agg *agg_id***[-***agg_id2***] size** *size* **[name** *name***] [admin-state {enable | disable}] [multi-chassis active] [hash {source-mac | destination-mac | source-and-destination-mac | source-ip | destination-ip | source-and-destination-ip | tunnel-protocol}]**

no linkagg static agg *agg_id***[-***agg_id2***]**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).
size	The maximum number of links allowed in the aggregate group.
name	The name of the static aggregate group. Can be any alphanumeric string. A group name with spaces must be contained within quotes (for example, “Static Group 1”).
enable	Specifies that the static aggregate group is active and is able to aggregate links.
disable	Specifies that the static aggregate group is inactive and not able to aggregate links.
multi-chassis active	*This parameter is not supported.*
source-mac	Selects the source MAC address hashing option.
destination-mac	Selects the destination MAC address hashing option.
source-and-destination-mac	Selects the source MAC address and destination MAC address hashing option.
source-ip	Selects the source IP hashing option.
destination-ip	Selects the destination IP hashing option.
source-and-destination-ip	Selects the source IP and destination IP hashing option.
tunnel-protocol	Selects the tunnel protocol (payload based) hashing option.

Defaults

parameter	default
enable | **disable**	enable
hash_option	**source-and-destination-IP** (Layer 3 traffic) **source-and-destination-mac** (Layer 2 traffic)

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a static aggregate group or a range of static aggregate groups from the configuration.
- Link aggregation cannot be configured on an AppMon enabled port.
- If the static aggregate has any attached ports. delete the attached ports with the **no** form of the **linkagg static port agg** command then remove the static link aggregate ID. Delete the attached ports using the **no linkagg static port** command.
- Specify the **hash** parameter option when the link aggregate is first created. The hashing algorithm options apply to unicast traffic and are not modifiable once the aggregate is created. If different options are required:
  - Disassociate all ports currently associated with the aggregate.
  - Delete the aggregate from the switch configuration.
  - Create the aggregate again with the new hashing options.
- It is not necessary to administratively down the linkagg ports before changing the hashing algorithm, but doing so is recommended to avoid any loss of traffic.
- The hashing algorithm does not take into consideration the speed of the ports to distribute the traffic. In other words, the same number of flows is distributed evenly on each port without consideration of the line speed.
- Aggregate load balancing is performed at the ingress side.
- Per-aggregate hashing is local to the switch, so each side of the aggregation can use different configurations for the hashing algorithms.
- Link aggregation follows the global hash control settings configured through the **hash-control brief** or **hash-control extended** commands.
- For example, when the **source-mac** option is specified for L2 hashing:
  - If the global hash-control is in brief mode, hashing is based on source MAC address only.
  - If the global hash-control is in extended mode, hashing is based on source MAC address, VLAN, Ethertype, and source module ID/port.
- For example, when the **source-ip** option is specified for L3 hashing:
  - If the global hash-control is in brief mode, hashing is based on source IP address only.
  - If the global hash-control is in extended mode, hashing is based on source IP address and source UDP-TCP Port.
- To load balance Unknown Destination/Broadcast/Multicast traffic on all the ports of the aggregate, use the **hash-control** command to enable load balancing of DFL traffic.
- Use the **linkagg lacp agg size** command to create a dynamic aggregation (LACP) group.

Examples

```
-> linkagg static agg 3-10 size 8
-> linkagg static agg 4 size 2 admin-state disable
-> linkagg static agg 4 size 2 hash source-and-destination-ip
-> no linkagg static agg 3-10
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; **tunnel-protocol** parameter added.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) link aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggSize
   alclnkaggAggLacpType
   alclnkaggAggName
   alclnkaggAggAdminState
   alclnkaggAggPortSelectionHash
```

linkagg static agg name

Configures a name for an existing static aggregate group.

linkagg static agg *agg_id***[-***agg_id2***] name** *name*

no linkagg static agg *agg_id***[-***agg_id2***] name**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).
name	The name of the static aggregation group, can be an alphanumeric string. A group name with spaces must be contained within quotes (for example, “Static Group 1”)

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a name from a static aggregate or from a range of static aggregates.
- You must assign names to static link aggregate IDs individually.
- To specify a range of link aggregates, use hyphen between the first and last link aggregate IDs of the range. A range of link aggregate IDs can be used only with the **no** form of this command.

Examples

```
-> linkagg static agg 2 name accounting
-> no linkagg static agg 2-10 name
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggName
```

linkagg static agg wait-to-restore-time

Configures the number of minutes to wait before bringing up a link aggregate that is attached to other link aggregates.

linkagg static agg *agg_id***[**-*agg_id2***] wait-to-restore-time** *wtr_minutes*

no linkagg static agg *agg_id***[**-*agg_id2***] wait-to-restore-time**

Syntax Definitions

*agg_id***[**-*agg_id2***]**	The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).
wtr_minutes	The number of minutes the switch waits to bring a link aggregate up. The range is 0–12 minutes.

Defaults

By default, the wait-to-restore timer is set to 0 (disabled).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the wait-to-restore timer for the specified link aggregate or aggregates.
- If a link aggregate is not attached to other links, this timer value is ignored and the aggregate is immediately brought up.

Examples

```
-> linkagg static agg 2 wait-to-restore-time 10
-> linkagg static agg 2 wait-to-restore-time 0
-> linkagg static agg 4 wait-to-restore-time 5
-> no linkagg static agg 4 wait-to-restore-time
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggWTRTimer
```

linkagg static agg loopback

Configures the specified link aggregate group to run in loopback mode. This is required if the link aggregate is going to provide loopback functionality to support L3 VPN inline routing for an IP over Shortest Path Bridging (SPB) configuration.

linkagg static agg *agg_id***[-***agg_id2***] loopback**

Syntax Definitions

*agg_id***[-***agg_id2***]**	An existing link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- Only front-panel ports that are also configured to run in loopback mode can be assigned to this type of link aggregate.
- Once the loopback mode is enabled for a link aggregate, the link aggregate is dedicated to providing loopback functionality for an SPB L3 VPN inline routing configuration. The loopback mode is disabled only when the link aggregate is deleted.
- Only one link aggregate per switch can be configured to run in loopback mode.
- For more information about SPB L3 VPN, see the “IP over SPBM” section of the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

Examples

```
-> linkagg static agg 2 loopback
-> linkagg static agg 10 loopback
ERROR: Internal Loopback aggregate already exists
```

Release History

Release 8.6R2; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
interfaces loopback	Configures a front-panel port to run in the loopback mode.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggLoopbackState
```

linkagg static agg loopback internal

Configures the specified link aggregate group to run in internal loopback mode. This is required if the link aggregate is going to provide loopback functionality to support L3 VPN inline routing for an IP over Shortest Path Bridging (SPB) configuration.

linkagg static agg *agg_id***[-***agg_id2***] loopback**

Syntax Definitions

*agg_id***[-***agg_id2***]**	An existing link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- When the internal loopback mode is enabled, internal ports are assigned to the link aggregate group. These ports are dedicated for this purpose; front-panel ports are not assigned to this type of link aggregate.
- No external cable is required and no front-panel ports are used up to provide the L3 VPN loopback functionality when internal loopback is used to define an L3 VPN gateway interface.
- Only one link aggregate per switch can be configured to run in the internal loopback mode.
- Once the internal loopback mode is enabled for a link aggregate, the link aggregate is dedicated to providing loopback functionality for an SPB L3 VPN inline routing configuration. The internal loopback mode is disabled only when the link aggregate is deleted.
- For more information about SPB L3 VPN, see the “IP over SPBM” section of the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide.*

Examples

```
-> linkagg static agg 2 loopback internal
-> linkagg static agg 10 loopback internal
ERROR: Internal Loopback aggregate already exists
```

Release History

Release 8.6R2; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggLoopbackState
```

linkagg static agg admin-state

Enables or disables the administrative state of a static link aggregation group.

linkagg static agg *agg_id***[**-*agg_id2***] admin-state {enable | disable}**

Syntax Definitions

*agg_id***[**-*agg_id2***]**	The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).
enable	Specifies that the static aggregate group is active and is able to aggregate links.
disable	Specifies that the static aggregate group is inactive and not able to aggregate links.

Defaults

parameter	default
enable | **disable**	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When the administrative state is set to **disable**, the static aggregate group is disabled.

Examples

```
-> linkagg static agg 2 admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggAdminState
```

linkagg static port agg

Configures a slot and port for a static aggregate group.

linkagg static port *chassis/slot/port***[**-*port2***] agg** *agg_id*

no linkagg static port *chassis/slot/port***[**-*port2***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
agg_id	The ID number corresponding to the static aggregate group.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove one or more ports from a static aggregate group.
- A port can belong to only one aggregate group.
- Ports that belong to the same static aggregate group need not be configured sequentially and can be on any Network Interface (NI).
- To specify a range of link aggregates, use hyphen between the first and last link aggregate IDs of the range. A range of link aggregate IDs can be used only with the **no** form of this command.

Examples

```
-> linkagg static port 2/1-5 agg 4
-> no linkagg static port 2/1-5
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
show linkagg port	Displays information about link aggregation ports.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortLacpType
   alclnkaggAggPortSelectedAggNumber
```

linkagg lacp agg size

Creates a dynamic aggregate group that uses the Link Aggregation Control Protocol (LACP) to establish and maintain link aggregation. The **size** parameter is required to create the link aggregate group.

linkagg lacp agg *agg_id***[-***agg_id2***] size** *size*
[name *name***]**
[admin-state {enable | disable}]
[actor admin-key *actor_admin_key***]**
[actor system-priority *actor_system_priority***]**
[actor system-id *actor_system_id***]**
[partner system-id *partner_system_id***]**
[partner system-priority *partner_system_priority***]**
[partner admin-key *partner_admin_key***]**
[multi-chassis active]
[hash {source-mac | destination-mac | source-and-destination-mac | source-ip | destination-ip | source-and-destination-ip | tunnel-protocol}]

no linkagg lacp agg *agg_id***[-***agg_id2***] size** *size*

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
size	The maximum number of links that can belong to the aggregate.
name	The name of the dynamic aggregate group. can be an alphanumeric string. A group name with spaces must be contained within quotes (for example, “Dynamic Group 1”).
enable	Specifies that the dynamic aggregate group is active and is able to aggregate links.
disable	Specifies that the dynamic aggregate group is inactive and not able to aggregate links.
actor_admin_key	The administrative key value associated with the dynamic aggregate group.
actor_system_priority	The priority of the dynamic aggregate group.
actor_system_id	The MAC address of the dynamic aggregate group on the switch.
partner_system_id	The MAC address of the aggregate group of the remote system which is attached to the aggregate group of the switch.
partner_system_priority	The priority of the remote system to which the aggregation group is attached.
partner_admin_key	The administrative key for the remote partner of the aggregation group.
source-mac	Selects the source MAC address hashing option.
destination-mac	Selects the destination MAC address hashing option.
source-and-destination-mac	Selects the source MAC address and destination MAC address hashing option.
source-ip	Selects the source IP hashing option.

destination-ip	Selects the destination IP hashing option.
source-and-destination-ip	Selects the source IP and destination IP hashing option.
tunnel-protocol	Selects the tunnel protocol hashing option.

Defaults

parameter	default
enable | disable	enable
hash_option	**source-and-destination-ip** (Layer 3 traffic) **source-and-destination-mac** (Layer 2 traffic)

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a dynamic aggregate group from the configuration.
- Link aggregation cannot be configured on an AppMon enabled port.
- You must disable the group with the **linkagg lacp agg admin-state** command before you can delete a dynamic link aggregate group.
- Optional parameters for the dynamic aggregate group can be configured when the aggregate is created. The dynamic aggregate group can be modified after the optional parameters are assigned.
- Specify the **hash** parameter option when the link aggregate is first created. The hashing algorithm options apply to unicast traffic and are not modifiable once the aggregate is created. If different options are required:
  - Disassociate all ports currently associated with the aggregate.
  - Delete the aggregate from the switch configuration.
  - Create the aggregate again with the new hashing options.
- It is not necessary to administratively down the linkagg ports before changing the hashing algorithm, but doing so is recommended.
- The hashing algorithm does not take into consideration the speed of the ports to distribute the traffic. In other words, the same number of flows is distributed evenly on each port without consideration of the line speed.
- Aggregate load balancing is performed at the ingress side.
- Per-aggregate hashing is local to the switch, so each side of the aggregation can use different configurations for the hashing algorithms.
- Link aggregation follows the global hash control settings configured through the **hash-control brief** or **hash-control extended** commands.
- For example, if the **source-mac** option is specified for L2 hashing:
  - If the global hash-control is in brief mode, hashing is based on source MAC address only.

  - If the global hash-control is in extended mode, hashing is based on source MAC address, VLAN, Ethertype, and source module ID/port.

- For example, if the **source-ip** option is specified for L3 hashing:
  - If the global hash-control is in brief mode, hashing is based on source IP address only.
  - If the global hash-control is in extended mode, hashing is based on source IP address and source UDP-TCP Port.
- To load balance Unknown Destination/Broadcast/Multicast traffic on all the ports of the aggregate, use the **hash-control** command to enable load balancing of DFL traffic.
- Use the **linkagg static agg size** command to create static aggregate groups. See page 12-3 for more information about this command.

Examples

```
-> linkagg lacp agg 2-5 size 4
-> linkagg lacp agg 3 size 2 admin-state disable actor system-priority 65535
-> no linkagg lacp agg 2-5 size 4
```

Release History

Release 7.1.1; command introduced.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggSize
   alclnkaggAggLacpType
   alclnkaggAggName
   alclnkaggAggAdminState
   alclnkaggAggActorAdminKey
   alclnkaggAggActorSystemPriority
   alclnkaggAggActorSystemID
   alclnkaggAggPartnerSystemID
   alclnkaggAggPartnerSystemPriority
   alclnkaggAggPartnerAdminKey
   alclnkaggAggPortSelectionHash
```

linkagg lacp agg name

Configures a name for a dynamic aggregate group.

linkagg lacp agg *agg_id* **name** *name*

no linkagg lacp agg *agg_id***[-***agg_id2***] name**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
name	The name of the dynamic aggregate group. Can be an alphanumeric string. A group name with spaces must be contained within quotes (for example, “Dynamic Group 1”).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a name from a single or a range of dynamic aggregate groups simultaneously.
- Assign names to individual dynamic link aggregate groups separately.

Examples

```
-> linkagg lacp agg 2 name finance
-> no linkagg lacp agg 2-5 name
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggName
```

linkagg lacp agg wait-to-restore-time

Configures the number of minutes to wait before bringing up a dynamic link aggregate that is attached to other link aggregates.

linkagg lacp agg *agg_id***[**-*agg_id2***]** **wait-to-restore-time** *wtr_minutes*

no linkagg lacp agg *agg_id***[**-*agg_id2***]** **wait-to-restore-time**

Syntax Definitions

*agg_id***[**-*agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
wtr_minutes	The number of minutes the switch waits to bring a link aggregate up. The range is 0–12 minutes.

Defaults

By default, the wait-to-restore timer is set to 0 (disabled).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the wait-to-restore timer for the specified link aggregate or aggregates.
- If a link aggregate is not attached to other links, this timer value is ignored and the aggregate is immediately brought up.

Examples

```
-> linkagg lacp agg 2 wait-to-restore-time 10
-> linkagg lacp agg 2 wait-to-restore-time 0
-> linkagg lacp agg 4 wait-to-restore-time 5
-> no linkagg lacp agg 4 wait-to-restore-time
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggWTRTimer
```

linkagg lacp agg admin-state

Configures the administrative state of a dynamic aggregate group or a range of dynamic aggregate groups.

linkagg lacp agg *agg_id***[**-*agg_id2***] admin-state {enable | disable}**

Syntax Definitions

*agg_id***[**-*agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
enable	Specifies that the dynamic aggregate group is active and is able to aggregate links.
disable	Specifies that the operation of a dynamic aggregate group cannot be performed.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the administrative state is set to **disable**, the operation of a dynamic aggregation (LACP) group cannot be performed.
- You can also enable or disable the admin-state for a range of link aggregate IDs simultaneously, using this command.

Examples

```
-> linkagg lacp agg 2 admin-state disable
-> linkagg lacp agg 2-10 admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregates.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggAdminState
```

linkagg lacp agg actor admin-key

Configures the administrative key associated with a dynamic aggregate group.

linkagg lacp agg *agg_id***[-***agg_id2***] actor admin-key** *actor_admin_key*

no linkagg lacp agg *agg_id***[-***agg_id2***] actor admin-key**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
actor_admin_key	The administrative key value associated with the dynamic aggregate group.

Defaults

parameter	default
actor_admin_key	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove an actor admin key from a dynamic aggregate group.

Examples

```
-> linkagg lacp agg 3-5 actor admin-key 2
-> no linkagg lacp agg 3-5 actor admin-key
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggActorAdminKey
```

linkagg lacp agg actor system-priority

Configures the priority of the dynamic aggregate group.

linkagg lacp agg *agg_id***[-***agg_id2***] actor system-priority** *actor_system_priority*

no linkagg lacp agg *agg_id***[-***agg_id2***] actor system-priority**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
actor_system_priority	The priority of the dynamic aggregate group of the switch in relation to other aggregate groups.

Defaults

parameter	default
actor_system_priority	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to return the value to its default.
- Ports with the same system priority value can join the same dynamic aggregate group.
- To assign or remove the actor system-priority for a series of link aggregate IDs, specify the range of link aggregate IDs with the **agg** keyword. Use a hyphen to separate the first and last link aggregate IDs of a range.

Examples

```
-> lacp linkagg 3 actor system-priority 100
-> no lacp linkagg 3 actor system-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggActorSystemPriority
```

linkagg lacp agg actor system-id

Configures the MAC address of a dynamic aggregate group on the switch.

linkagg lacp agg *agg_id***[-***agg_id2***] actor system-id** *actor_system_id*

no linkagg lacp agg *agg_id***[-***agg_id2***] actor system-id**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
actor_system_id	The MAC address of the dynamic aggregate group on the switch in the hexadecimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
actor_system_id	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the MAC address assignment (actor system ID) from a dynamic link aggregate or a range of dynamic link aggregates simultaneously.
- You can configure the MAC address for a range of dynamic link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range along with this command.

Examples

```
-> linkagg lacp agg 2 actor system-id 00:20:da:81:d5:b0
-> no linkagg lacp agg 3-10 actor system-id
-> no linkagg lacp agg 11 actor system-id
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggActorSystemID
```

linkagg lacp agg partner system-id

Configures the MAC address of the dynamic aggregate group of the remote system that is attached to the dynamic aggregate group of the local switch.

linkagg lacp agg *agg_id***[-***agg_id2***] partner system-id** *partner_system_id*

no linkagg lacp agg *agg_id***[-***agg_id2***] partner system-id**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
partner_system_id	The MAC address of the dynamic aggregate group of the remote switch in the hexadecimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
partner_system_id	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a partner system ID from a dynamic aggregate group or a range of groups assigned with the same partner system IDs together.
- The *partner_system_id* and the *partner_system_priority* together specify the priority of the remote system.
- You can configure a partner system ID for a range of dynamic link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range along with this command.

Examples

```
-> linkagg lacp agg 2 partner system-id 00:20:da4:32:81
-> linkagg lacp agg 2-10 partner system-id 00:20:da4:32:82
-> no linkagg lacp agg 2-10 partner system-id
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggPartnerSystemID
```

linkagg lacp agg partner system-priority

Configures the priority of the dynamic aggregate group of the remote system which is attached to the dynamic aggregate group of the local switch.

linkagg lacp agg *agg_id***[-***agg_id2***] partner system-priority** *partner_system_priority*

no linkagg lacp agg *agg_id***[-***agg_id2***] partner system-priority**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
partner_system_priority	The priority of the dynamic aggregate group of the remote system which is attached to the dynamic aggregate group of the local switch.

Defaults

parameter	default
partner_system_priority	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to return to the priority value to its default.
- The *partner_system_id* and the *partner_system_priority* together specify the priority of the remote system.
- You can apply the partner system-priority to a range of link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range after the **agg** keyword.

Examples

```
-> linkagg lacp agg 3 partner system-priority 65535
-> linkagg lacp agg 3-6 partner system-priority 65535
-> no linkagg lacp agg 3-6 partner system-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggPartnerSystemPriority
```

linkagg lacp agg partner admin-key

Configures the administrative key for the remote partner of the dynamic aggregation group.

linkagg lacp agg *agg_id***[-***agg_id2***] partner admin-key** *partner_admin_key*

no linkagg lacp agg *agg_id***[-***agg_id2***] partner admin-key**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
partner_admin_key	The administrative key for the remote partner of the dynamic aggregation group.

Defaults

parameter	default
partner_admin_key	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a partner admin-key from a dynamic aggregate group.
- The partner admin-key can be assigned for a range of dynamic link aggregate IDs simultaneously.

Examples

```
-> linkagg lacp agg 3-5 partner admin-key 3
-> no linkagg lacp agg 3-10 partner admin-key
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggPartnerAdminKey
```

linkagg lacp port actor admin-key

Configures an actor administrative key for a port, which allows the port to join a dynamic aggregate group.

linkagg lacp port *chassis/slot/port***[**-*port2***]** **actor admin-key** *actor_admin_key*
[actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}]
[actor system id *actor_system_id***]**
[actor system priority *actor_system_priority***]**
[partner admin system id *partner_admin_system_id***]**
[partner admin-key *partner_admin_key***]**
[partner admin system priority *partner_admin_system_priority***]**
[partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}]
[actor port priority *actor_port_priority***]**
[partner admin port *partner_admin_port***]**
[partner admin port priority *partner_admin_port_priority***]**

no linkagg lacp port *chassis/slot/port***[**-*port2***] [actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}]**
[actor system id *actor_system_id***]**
[actor system priority *actor_system_priority***]**
[partner admin system id *partner_admin_system_id***]**
[partner admin-key *partner_admin_key***]**
[partner admin system priority *partner_admin_system_priority***]**
[partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}]
[actor port priority *actor_port_priority***]**
[partner admin port *partner_admin_port***]**
[partner admin port priority *partner_admin_port_priority***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
actor_admin_key	The administrative key associated with this dynamic aggregate group.
actor admin-state	See the **linkagg lacp port actor admin-state** command.
actor_system_id	The MAC address of this dynamic aggregate group on the switch.
actor_system_priority	The priority of the dynamic aggregate group.
partner_admin_system_id	The MAC address of the dynamic aggregate group of the remote switch.
partner_admin_key	The administrative key for the remote partner of the dynamic aggregation group.

partner_admin_system_priority	The priority of the remote system to which the dynamic aggregation group is attached.
partner admin-state	See the **linkagg lacp agg partner admin-state** command.
actor_port_priority	The priority of the actor port.
partner_admin_port	The administrative state of the partner port.
partner_admin_port_priority	The priority of the partner port.

Defaults

parameter	default
[active] [timeout]....	active, timeout, aggregate

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a slot and port from a dynamic aggregate group.
- A port can belong to only one aggregate group.
- Ports that belong to a dynamic link aggregate must be configured to the same link speed.
- Ports that belong to the same dynamic aggregate group need not be configured sequentially and can be on any Network Interface (NI).

Examples

```
-> linkagg lacp agg 3/1 actor admin-key 0
-> no linkagg lacp agg 3/1 actor admin-key
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregates.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggActorAdminKey
   alclnkaggAggPortLacpType
   alclnkaggAggPortActorAdminState
   alclnkaggAggPortActorSystemID
   alclnkaggAggPortActorSystemPriority
   alclnkaggAggPortPartnerAdminSystemID
   alclnkaggAggPortPartnerAdminKey
   alclnkaggAggPortPartnerAdminSystemPriority
   alclnkaggAggPortPartnerAdminState
   alclnkaggAggPortActorPortPriority
   alclnkaggAggPortPartnerAdminPort
   alclnkaggAggPortPartnerAdminPortPriority
```

linkagg lacp port actor admin-state

Configures the system administrative state of the slot and port for the dynamic aggregate group on the local switch. The state values correspond to bits in the actor state octet in the LACPDU frame.

linkagg lacp port *chassis/slot/port***[**-*port2***] actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}**

no linkagg lacp port *chassis/slot/port***[**-*port2***] actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
active	Specifies that bit 0 in the actor state octet is enabled. When this bit is set, the dynamic aggregate group is able to exchange LACPDU frames. By default, this value is set.
timeout	Specifies that bit 1 in the actor state octet is enabled. When this bit is set, a short timeout is used for LACPDU frames. When this bit is disabled, a long timeout is used for LACPDU frames. By default, this value is set.
aggregate	Specifies that bit 2 in the actor state octet is enabled. When this bit is set, the system considers this port to be a potential candidate for aggregation. If this bit is not enabled, the system considers the port to be individual (it can only operate as a single link). By default, this value is set.
synchronize	Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 3) is set by the system, the port is allocated to the correct dynamic aggregation group. If this bit is not set by the system, the port is not allocated to the correct dynamic aggregation group.
collect	Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 4) is set by the system, incoming LACPDU frames are collected from the individual ports that make up the dynamic aggregate group.
distribute	Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 5) is set by the system, distributing outgoing frames on the port is disabled.
default	Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 6) is set by the system, it indicates that the actor is using the defaulted partner information administratively configured for the partner.
expire	Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 7) is set by the system, the actor cannot receive LACPDU frames.
none	Resets all administrative states to their default configurations.

Defaults

parameter	default
[active] [timeout]....	active, timeout, aggregate
timeout enable	Disabled (OmniSwitch 9900) Enabled (All other platforms)

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the LACPDU bit settings to their default configuration.
- When the actor admin-state is set to **none**, all bit values are restored to their default configurations.
- Enabling the **timeout** parameter configures a 1 second interval (short timeout / fast transmit rate). Disabling the **timeout** parameter configures a 30 second interval (long timeout / slow transmit rate).
- **timeout** option when used sets only the transmit rate. The remote side timeout is 3X the configured transmit rate. For example, if the transmit rate is set to 1 packet per second, the remote side will timeout if it misses 3 packets. In this case, it will timeout in 3 seconds. If the transmit rate is set to 30 packets per second, then the remote side will take 90 seconds to timeout.
- 'no linkagg lacp port actor admin-state timeout' disables the **timeout** parameter, which results in a long timeout, that is, 30 second transmission rate.

Examples

```
-> linkagg lacp port 4/2 actor admin-state synchronize collect distribute
-> no linkagg lacp port 4/2 actor admin-state synchronize collect
-> linkagg lacp port 4/2 actor admin-state none
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortActorAdminState
```

linkagg lacp port actor system-id

Configures the system ID (i.e., MAC address) for the local port associated with a dynamic aggregate group.

linkagg lacp port *chassis/slot/port***[**-*port2***] actor system-id** *actor_system_id*

no linkagg lacp port *chassis/slot/port***[**-*port2***] actor system-id**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
actor_system_id	The MAC address of the dynamic aggregate group on the switch in the hexadecimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
actor_system_id	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the actor system ID from a slot and port or a range of slot and ports associated with a dynamic aggregate group.
- Configure the system ID for a range of local ports simultaneously. Use a hyphen to separate the first and last port IDs of a range after the **port** keyword.

Examples

```
-> linkagg lacp port 3/1-10 actor system-id 00:20:da:06:ba:d3
-> no linkagg lacp port 3/1-10 actor system-id
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortActorSystemID
```

linkagg lacp port actor system-priority

Configures the system priority of the port on the switch that belongs to the dynamic aggregate group.

linkagg lacp port *chassis/slot/port***[**-*port2***] actor system-priority** *actor_system_priority*

no linkagg lacp port *chassis/slot/port***[**-*port2***] actor system-priority**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
actor_system_priority	The priority of the dynamic aggregate group.

Defaults

parameter	default
actor_system_priority	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an actor system priority value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.
- Configure the actor system-priority to a range of ports simultaneously. Use a hyphen to separate the first and last port of a range after the **port** keyword.

Examples

```
-> linkagg lacp port 3/2-10 actor system-priority 65
-> no linkagg lacp port 3/2-10 actor system-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregates.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortActorSystemPriority
```

linkagg lacp agg partner admin-state

Configures the system administrative state of the slot and port for the dynamic aggregate group on the remote switch. The state values correspond to bits in the actor state octet in the LACPDU frame.

linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}**

no linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
active	Specifies that bit 0 in the partner state octet is enabled. When this bit is set, the dynamic aggregate group is able to exchange LACPDU frames. By default, this value is set.
timeout	Specifies that bit 1 in the partner state octet is enabled. When this bit is set, a short timeout is used for LACPDU frames. When this bit is disabled, a long timeout is used for LACPDU frames. By default, this value is set.
aggregate	Specifies that bit 2 in the partner state octet is enabled. When this bit is set, the system considers this port to be a potential candidate for aggregation. If this bit is not enabled, the system considers the port to be individual (it can only operate as a single link). By default, this value is set.
synchronize	Specifies that bit 3 in the partner state octet is enabled. When this bit is set, the port is allocated to the correct dynamic aggregation group. If this bit is not enabled, the port is not allocated to the correct aggregation group. By default, this value is disabled.
collect	Specifying this keyword has no effect because the system always determines its value. When this bit (bit 4) is set by the system, incoming LACPDU frames are collected from the individual ports that make up the dynamic aggregate group.
distribute	Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 5) is set by the system, distributing outgoing frames on the port is disabled.
default	Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 6) is set by the system, it indicates that the partner is using the defaulted actor information administratively configured for the actor.
expire	Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 7) is set by the system, the partner cannot receive LACPDU frames.
none	Resets all administrative states to their default configurations.

Defaults

parameter	default
[active] [timeout]	active, timeout, aggregate
timeout enable	Disabled (OmniSwitch 9900) Enabled (All other platforms)
timeout enable	Disabled (OmniSwitch 9900) Enabled (All other platforms)

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the LACPDU bit settings to their default configuration for a single port or a range of ports.
- When the partner admin-state is set to **none**, all bit values are restored to their default configurations.
- Configure the system administrative state for a range of ports simultaneously. Use a hyphen to separate the first and last port of a range after the **port** keyword.
- Enabling the **timeout** parameter configures a 1 second interval (short timeout / fast transmit rate). Disabling the **timeout** parameter configures a 30 second interval (long timeout / slow transmit rate).
- **timeout** option when used sets only the transmit rate. The remote side timeout is 3X the configured transmit rate. For example, if the transmit rate is set to 1 packet per second, the remote side will timeout if it misses 3 packets. In this case, it will timeout in 3 seconds. If the transmit rate is set to 30 packets per second, then the remote side will take 90 seconds to timeout.
- 'no linkagg lacp port partner admin-state' disables the **timeout** parameter, which results in a long timeout, that is, 30 second transmission rate.

Examples

```
-> lacp port 4/2-10 partner admin-state synchronize collect distribute
-> no lacp agg 4/2-10 partner admin-state synchronize collect
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminState
```

linkagg lacp port partner admin system-id

Configures the partner administrative system ID for a dynamic aggregate group port.

linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin system-id** *partner_admin_system_id*

no linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin system-id**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
partner_admin_system_id	The MAC address of the remote dynamic aggregate group in the hexadecimal format *xx:xx:xx:xx:xx:xx*.

Defaults

parameter	default
partner_admin_system_id	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove a partner administrative system ID from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 3/1-10 partner admin system-id 00:20:da:05:f6:23
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminSystemID
```

linkagg lacp port partner admin-key

Configures the partner administrative key for a dynamic aggregate group port.

linkagg lacp port *chassis/slot/port***[-***port2***] partner admin-key** *partner_admin_key*

no linkagg lacp port *chassis/slot/port***[-***port2***] partner admin-key**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
partner_admin_key	The administrative key for the remote partner of a dynamic aggregation group.

Defaults

parameter	default
partner_admin_key	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove a partner admin key value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 partner admin-key 0
-> no linkagg lacp port 2/1-5 partner admin-key
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminKey
```

linkagg lacp port partner admin system-priority

Configures the partner system priority for a dynamic aggregate group port.

linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin system-priority** *partner_admin_system_priority*

no linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin system-priority**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
partner_admin_system_priority	The priority of the dynamic aggregate group of the remote switch to which the aggregation group is attached.

Defaults

parameter	default
partner_admin_system_priority	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove a *partner_system_priority* value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 partner admin system-priority 65
-> no linkagg lacp port 2/1-5 partner admin system-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortAdminSystemPriority
```

linkagg lacp port actor port priority

Configures the priority for an actor port.

linkagg lacp port *chassis/slot/port***[**-*port2***] actor port-priority** *actor_port_priority*

no linkagg lacp port *chassis/slot/port***[**-*port2***] actor port-priority**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
actor_port_priority	The priority of the actor port.

Defaults

parameter	default
actor_port_priority	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove an *actor_port_priority* value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 actor port-priority 100
-> no linkagg lacp port 2/1-5 actor port-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortActorPortPriority
```

linkagg lacp port partner admin-port

Configures the administrative status of a partner port.

linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin-port** *partner_admin_port*

no linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin-port**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
partner_admin_port	The administrative state of the partner port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove a *partner_admin_port* value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 partner admin-port 255
-> no linkagg lacp port 2/1-5 partner admin-port
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminPort
```

linkagg lacp port partner admin port-priority

Configures the priority for a partner port.

linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin port-priority** *partner_admin_port_priority*

no linkagg lacp port *chassis/slot/port***[**-*port2***] partner admin port-priority**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
partner_admin_port_priority	The priority of the partner port.

Defaults

parameter	default
partner_admin_port_priority	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove a *partner_admin_port_priority* value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 partner admin port-priority 100
-> no linkagg lacp port 2/1-5 partner admin port-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminPortPriority
```

dhl name

Configures a Dual-homed Link (DHL) session associated with the specified session ID number.

dhl *dhl_num* **[name** *name***]**

no dhl *dhl_num*

Syntax Definitions

dhl_num	The DHL session ID number. Valid range is 1–1000.
name	The name of the DHL session.

Defaults

By default, if a name is not assigned to a DHL session, the session is configured as DHL-1.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- Use the **no** form of this command to remove a DHL session ID from the switch configuration.
- Use the optional **name** parameter to specify a name for the DHL session.
- Only one DHL session can be configured on a switch.
- Once the DHL session ID is created, assign a link A port and a link B port to the session. This is required before administratively enabling the DHL session is allowed.

Examples

```
-> dhl 1 name dhl_session1
-> no dhl 1
```

Release History

Release 8.2.1; command was introduced.

Related Commands

dhl linka linkb	Associates a pair of links (port or linkagg) with the DHL session.
dhl admin-state	Configures the administrative status of the DHL session.
show dhl	Displays information about a specific DHL session.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionIndex
   alaDHLSessionDescr
```

dhl linka linkb

Configures two ports or two link aggregates or a combination of both as linkA and linkB for the specified DHL session. Only two links are allowed per DHL session; only one DHL session per switch is allowed.

dhl *dhl_num* **linka {port** *chassis/slot/port* **| linkagg** *agg_id***} linkb {port** *chassis/slot/port* **| linkagg** *agg_id***}**

no dhl *dhl_num* **linka {port** *chassis/slot/port* **| linkagg** *agg_id***} linkb {port** *chassis/slot/port* **| linkagg** *agg_id***}**

Syntax Definitions

dhl_num	An existing DHL session ID number.
chassis	The chassis ID number.
slot	The slot number to designate as a link for the DHL session.
port	The physical port number to designate as a link for the DHL session.
agg_id	The link aggregate ID number to designate as a link for the DHL session.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- Use the **no** form of this command to remove the linkA and linkB ports from the specified session ID. Before attempting to remove the links, administratively disable the DHL session.
- Make sure that DHL linkA and linkB are associated with each of the VLAN that the DHL session will protect. Any VLAN not associated with both the links or only associated with one of the links is unprotected.
- DHL linkA *and* linkB should belong to the same default VLAN. In addition, select a default VLAN that is one of the VLANs that the DHL session will protect. For example, if the session is going to protect VLANs 10-20, then assign one of those VLANs as the default VLAN for linkA and linkB.
- Only one DHL session per switch is allowed. Each session can have only two links (linkA and linkB). Specify a physical switch port or a link aggregate (linkagg) ID as a DHL link. The same port or link aggregate is not configurable as both linkA or linkB.
- DHL is not supported on mobile, 802.1x-enabled, GVRP, or UNI ports. DHL is also not supported on a port that is a member of a link aggregate or a port the is enabled for transparent bridging.
- The administrative state of a DHL session is not configurable until a linkA port and a linkB port are associated with the specified DHL session ID number.
- Changing the port designations for linkA and linkB is not recommended while the DHL session is enabled.

- Removing a link aggregate from the switch configuration is not allowed if the aggregate is configured as a link for a DHL session.

Examples

```
-> dhl 1 linka port 1/1 linkb port 1/2
-> dhl 1 linka  linkagg 1  linkb port 1/2
-> dhl 1 linka port 1/1 linkb linkagg 1
-> dhl 1 linka  linkagg 1  linkb linkagg 2
-> no dhl 1 linka port 1/1 linkb port 1/2
```

Release History

Release 8.2.1; command was introduced.

Related Commands

dhl name	Configures a session ID for the DHL session.
dhl admin-state	Configures the administrative status for the DHL session.
show dhl	Displays the global status of the DHL configuration.
show dhl	Displays information about a specific DHL session.
show dhl link	Displays information about a specific link.

MIB Objects

```
AlaDHLLinksTable
   alaDHLLinksSessionIndex
   alaDHLLinkslinkA
   alaDHLLinkslinkB
```

dhl admin-state

Enables or disables the administrative state of a DHL session.

dhl *dhl_num* **admin-state {enable | disable}**

Syntax Definitions

dhl_num	An existing DHL session ID number.
enable	Enables the DHL session.
disable	Disables the DHL session.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- The DHL session ID specified with this command must already exist in the switch configuration.
- The administrative state cannot be enabled until a linkA port and a linkB port are associated with the specified DHL session ID number.

Examples

```
-> dhl 1 admin-state enable
-> dhl 1 admin-state disable
```

Release History

Release 8.2.1; command was introduced.

Related Commands

dhl name	Configures a session ID for the DHL session.
dhl admin-state	Configures the administrative status for the DHL session.
show dhl	Displays the global status of the DHL configuration or information about a specific DHL session.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionAdminStatus
```

dhl vlan-map linkb

Configures a VLAN-MAP (a single VLAN or a range of VLANs) from a common pool of VLANs to operate on DHL link B.

dhl *dhl_num* **vlan-map linkb {***vlan_id***[-***vlan_id***]}**

no dhl *dhl_num* **vlan-map linkb {***vlan_id***[-***vlan_id***]}**

Syntax Definitions

dhl_num	A DHL session ID number.
*vlan_id***[-***vlan_id***]**	A VLAN ID number or a range of VLAN IDs to map to linkB. The valid range is 1–4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- A DHL session has to be created before a VLAN-MAP can be configured.
- When the DHL session is active, the common VLAN that both the dual homed links belong to is treated as a protected VLAN. The VLAN containing only one dual homed link is treated as an unprotected VLAN. Traffic is forwarded only on the dual homed links belonging to the protected VLAN.
- If a VLAN is removed globally and if the VLAN belongs to a particular dual homed link, then the VLAN will automatically be removed from the dual homed link.
- If one dual homed link, for example linkA, is moved out of a protected VLAN, then the VLAN becomes unprotected and the VPA is removed from the second dual homed link, for example linkB.
- If the admin state of a VLAN is changed to disabled, and if the VLAN is part of a protected VLAN, then the disabled VLAN is removed from the operational DHL VLAN list but will be present in the protected VLAN list.
- If the admin state of a dual homed link, for example linkA, is changed to disabled, then the protected VLANs of the disabled linkA are moved to the other link, for example linkB. When linkA is re-enabled, then the VLANs are moved back to linkA.
- If the VLAN-MAP of linkB is removed, then the VPAs for the linkB will also be removed and the VLANs configured on linkB are moved to linkA.
- If a VLAN is configured as default on one dual homed link, for example linkA, then the same VLAN cannot be configured as tagged on the other link, for example linkB.

Examples

```
-> vlan 10-30
-> vlan 10-20 802.1q 1/1
-> vlan 4
-> vlan port default 1/1-2
-> dhl 1 name dhl_session1
-> dhl 1 linka port 1/1 linkb port 1/2
-> dhl 1 vlan-map linkb 18-20
-> no dhl 1 vlan-map linkb 18-20
```

Release History

Release 8.2.1; command was introduced.

Related Commands

dhl name	Configures a session ID for the DHL session.
dhl admin-state	Configures the administrative status for the DHL session.
show dhl	Displays the global status of the DHL configuration or information about a specific DHL session.
show dhl link	Displays information about a specific link.

MIB Objects

```
alaDHLVlanMapTable
   alaDHLVlanMapSessionIndex
   alaDHLVlanMapVlanStart
   alaDHLVlanMapVlanEnd
   alaDHLVlanMapRowStatus
```

dhl pre-emption-time

Configures the pre-emption timer for the DHL session. A pre-emption timer is a recovery-delay timer that is used to delay the switchover of VLANs to their primary links. It is the delay in the resumption of traffic when a link that is down is brought up.

dhl *dhl_num* **pre-emption-time** *seconds*

Syntax Definitions

dhl_num	A DHL session ID number.
seconds	The number of seconds for the delay in the switchover of VLANs to their primary links. The valid range is 0–600.

Defaults

parameter	default
seconds	30 seconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- Pre-emption timer is applicable only when a failed port is brought up. If both ports are down, the pre-emption timer is activated only when the second port is brought up.
- If the pre-emption timer value is set to 0, then there will be no delay in the VLANs being moved back to their primary link.
- If a link fails when the pre-emption timer is active, that is when the remaining pre-emption time value is not equal to 0, then the timer will be halted.
- When the pre-emption timer is active for a particular link and if the other link goes down, then the VLANs of the link that is down are automatically moved to the port for which the pre-emption timer is active.
- When DHL ports spanned across the NIs or DHC ports are on the same NI but data port is on different NI, it is advised to configure mac-flush mechanism (either Raw/MVRP) for faster convergence.

Examples

```
-> dhl 1 pre-emption-time 40sec
```

Release History

Release 8.2.1; command was introduced.

Related Commands

dhl name	Configures a session ID for the DHL session.
show dhl	Displays the global status of the DHL configuration or information about a specific DHL session.
show dhl link	Displays information about a specific link.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionPreemptionTime
```

dhl mac-flushing

Configures the MAC-flushing technique for the DHL session. The MAC-flushing technique is used to correct any stale MAC entries that are caused when a dual homed link goes down.

dhl *dhl_num* **mac-flushing {none | raw | mvrp}**

Syntax Definitions

dhl_num	A DHL session ID number.
none	Flushing of the MAC address tables does not occur.
raw	Method of flushing when VPAs of the links moved across them due to link up/down or configuration change (VLAN-map). The switch determines the MAC addresses within the affected VLANs
mvrp	Method of flushing when one link fails and the other link issues 'join' declarations to establish connectivity. These new joins are flagged as 'new' and they are forwarded by the core devices causing flushing on the core network for the active VLANs.

Defaults

parameter	default
none | raw | mvrp	**none**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- Before enabling MVRP on dual homed links, the Registrar Mode should be set to 'forbidden', failing which an error message is displayed when configuring DHL. If the Registrar Mode is set to 'not forbidden, then changes cannot be made to the MVRP configuration on the dual homed links.
- If the MAC-flushing technique is set to MVRP and if MVRP is not enabled on the dual homed links, then the **show dhl** command displays the active MAC-flushing technique as **none**. When MVRP is enabled on the dual homed links, then the MAC-flushing technique changes to **MVRP** and the Registrar Mode of the links is automatically set to ‘forbidden’.
- If VLANs are moved across the dual homed links as a result of configuration changes, then MAC-flushing is automatically enabled, if configured, excepting dual homed links that are changed on the fly.

Examples

```
-> dhl 1 mac-flushing none
-> dhl 1 mac-flushing raw
```

Release History

Release 8.2.1; command was introduced.

Related Commands

dhl name	Configures a session ID for the DHL session.
show dhl	Displays the global status of the DHL configuration or information about a specific DHL session.
show dhl link	Displays information about a specific link.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionMacFlushingtech
```

show dhl

Displays the global status of the DHL configuration or information about a specific DHL session.

show dhl [*dhl_num***]**

Syntax Definitions

dhl_num	A DHL session ID number.

Defaults

By default, the global status of the DHL configuration is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

Use the *dhl_num* parameter to display information about a specific DHL session.

Examples

```
-> show DHL
 Number  Name   Admin    Oper     Pre-emption    Mac-flushing   Active Mac-flushing
                state    state    time
-------+------+--------+-------+-----------+-----------------+--------------------
  1      DHL-1   UP       UP      30sec          Raw                Raw
```

output definitions

Number	Number of the DHL session.
Name	The user-defined text description of the DHL session.
Admin state	The administrative status of the DHL session.
Oper state	The operational status of the DHL session.
Pre-emption time	The pre-emption time in seconds of the DHL session.
Mac-flushing	Mac-flushing technique on the DHL session.
Active Mac-flushing	Mac-flushing technique that is currently active on the DHL session.

```
-> show dhl 1
DHL session name              : Arice,
Admin state                   : Up,
Operational state             : Up,
Pre-emption time              : 40 sec,
Mac-flushing                  : Raw-Flushing,
Active Mac-flushing           : Raw-Flushing,

Protected VLANs               : 10-20,23,25,30-100,600,700,800,

linkA:
```

```
  Port                        : 1/2,
  Operational state           : Up

  Un protected VLANs           : 900,1980,1987,234,
  Active VLAN                 : 10-20,23,25,30-100,600,700,800,

linkB:
  Port                        : 1/1,
  Operational state           : Down,
  Un protected VLANs          : 1730-1800,
  Vlan-map                    : 30-100,600,
  Active Vlans                :  none,
```

output definitions

DHL session Name	The user-defined text description of the DHL session.
Admin state	The current administrative status of the DHL session.
Operational state	The operational state of the DHL session.
Pre-emption time	The delay-interval in seconds to move the VLANs back to their original links.
Mac-flushing	Mac-flushing technique on the DHL session.
Active Mac-flushing	The active Mac-flushing technique that is enabled on the specified DHL session.
Protected VLANs	The common VLANs that contain both the dual homed links, for example linkA and linkB.
LinkA	A dual homed link that is part of a pair of DHL links that can be configured per switch.
Port	The port number of linkA.
Operational state	The operational state of the port. The operational states are UP or DOWN.
Un protected VLANs	The VLANs containing only one dual homed link.
Active VLANs	The VLANs that are in an active state.
LinkB	A dual homed link that is part of a pair of DHL links that can be configured per switch.
Port	The port number of linkB.
Operational state	The operational state of the port. The operational states are UP or DOWN.
Un protected VLANs	The VLANs containing only one dual homed link.
VLAN-map	The DHL VLAN map for linkB. This specifies the VLANs that are operational on DHL linkB from the common pool of VLANs between DHL linkA and linkB.
Operational VLANs	The VLANs that are in an operational state.

Release History

Release 8.2.1; command was introduced.

Related Commands

dhl name	Configures a session ID for the DHL session.
show dhl link	Displays information about a specific link.

MIB Objects

```
alaDHLSessionTable
   alaDHLSessionIndex
   alaDHLSessionDesc
   alaDHLSessionAdminStatus
   alaDHLSessionOperStatus
   alaDHLSessionPreemptionTime
   alaDHLSessionMacFlushingtech
alaDHLLinksTable
   alaDHLLinksSessionIndex
   alaDHLLinkslinkA
   alaDHLLinkslinkAOperStatus
   alaDHLLinkslinkB
   alaDHLLinkslinkBOperStatus
alaDHLVlanMapTable
   alaDHLVlanMapSessionIndex
   alaDHLVlanMapVlanStart
   alaDHLVlanMapVlanEnd
alaDHLVpaTable
   alaDHLVpalink
   alaDHLVpaVlan
   alaDHLVpaVlanType
   alaDHLVpaOperationalLink
```

show dhl link

Displays information about a specific DHL link, for example linkA or linkB and the VLAN details of the specified link.

show dhl *dhl_num* **[linkA | linkB]**

Syntax Definitions

dhl_num	A DHL session ID number.
linkA	The dual homed link that is part of a pair of DHL links that can be configured per switch.
linkB	The dual homed link that is part of a pair of DHL links that can be configured per switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

N/A

Examples

```
-> show dhl 1 linkA

linkA:
  Port                        : 1/2,
  Operational state           : Up,

  Protected VLANs             : 10-20, 23, 25, 30-100,600,700,800,
  Un protected VLANs          : 900, 1980, 1987,234,
  Active VLAN                 : 10-20, 23, 25, 30-100,600,700,800,
```

Release History

Release 8.2.1; command was introduced.

Related Commands

dhl name	Configures a session ID for the DHL session.
dhl linka linkb	Configures a port or a link aggregate as dual homed links (linkA, linkB) of a DHL session.
dhl vlan-map linkb	Configures a VLAN or a range of VLANs from a common pool to operate on DHL linkB.
show dhl	Displays information about a specific DHL session.

MIB Objects

```
alaDHLLinksTable
   alaDHLLinksSessionIndex
   alaDHLLinkslinkA
   alaDHLLinkslinkAOperStatus
   alaDHLLinkslinkB
alaDHLVpaTable
   alaDHLVpalink
   alaDHLVpaVlan
   alaDHLVpaVlanType
   alaDHLVpaOperationalLink
alaDHLVlanMapTable
   alaDHLVlanMapSessionIndex
   alaDHLVlanMapVlanStartala
   alaDHLVlanMapVlanEnd
```

linkagg range

Modifies the range of standard and MC-LAG link aggregation identifiers.

linkagg range local {*agg_id-agg_id* | **none**} **peer** {*agg_id-agg_id* | **none**} **multi-chassis** {*agg_id-agg_id* | **none**}

Syntax Definitions

agg_id-agg_id	The first or last identifier in the range.
local	The range of standard local aggregate identifiers.
peer	The range of standard peer aggregate identifiers.
multi-chassis	The range of MC-LAG aggregate identifiers.
none	No aggregate identifiers range is specified.

Defaults

parameter	default
local	0-47
peer	48-95
multi-chassis	96-127

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command in conjunction with the MC-LAG feature to change the maximum number of MC-LAG link aggregates that can be configured.
- The switch must be rebooted for the ranges to take affect.
- The maximum number of combined standard and MC-LAG link aggregates is 128.

Examples

```
-> linkagg range local 0-9 peer 10-19 multi-chassis 20-127
-> linkagg range local none peer none multi-chassis 0-127
```

Release History

Release 7.1.1; command introduced.

Related Commands

show linkagg range	Displays the link aggregate ranges.

MIB Objects

```
alclnkaggAggConfig
   alclnkAggLocalRangeOperMin
   alclnkAggLocalRangeOperMax
   alclnkAggLocalRangeConfiguredMin
   alclnkAggLocalRangeConfiguredMax
   alclnkAggPeerRangeOperMin
   alclnkAggPeerRangeOperMax
   alclnkAggPeerRangeConfiguredMin
   alclnkAggPeerRangeConfiguredMax
   alclnkAggMcLagRangeOperMin
   alclnkAggMcLagRangeOperMax
   alclnkAggMcLagRangeConfiguredMin
   alclnkAggMcLagRangeConfiguredMax
```

show linkagg

Displays information about static and dynamic (LACP) aggregate groups.

show linkagg [agg *agg_id***[-***agg_id2***]]**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the aggregate group. Configured through the **linkagg static agg size** or **linkagg lacp agg size** command. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, information for all aggregate groups is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If an aggregate number is specified, only the information about the relevant aggregate group is displayed. The fields included in the display depend on whether the aggregate group is static or dynamic.
- Use the **show linkagg port** command to display information about aggregate group ports.

Examples

No aggregate group is specified:

```
-> show linkagg

Number  Aggregate     SNMP Id   Size Admin State  Oper State     Att/Sel Ports
-------+-------------+---------+----+------------+--------------+-------------
   1     Static       40000001   8   ENABLED      UP              2   2
   2     Dynamic      40000002   4   ENABLED      DOWN            0   0
   3     Dynamic      40000003   8   ENABLED      DOWN            0   2
   4     Dynamic      40000004   8   ENABLED      UP              3   3
   5     Static       40000005   2   DISABLED     DOWN            0   0
  10     Loopback     40000010   2   ENABLED      DOWN            0   0
```

output definitions

Number	The aggregate group number.
Aggregate	The type of aggregate group (**Static**, **Dynamic**, or **Loopback**).
SNMP Id	The SNMP ID associated with the aggregate group.
Size	The number of links in this aggregate group.

output definitions (continued)

Admin State	The current administrative state of the aggregate group (**ENABLED** or **DISABLED**). Configured through the **linkagg static agg admin-state** command for static aggregate groups and the **linkagg lacp agg admin-state** command for dynamic aggregate groups.
Oper State	The current operational state of the aggregate group (**UP** or **DOWN**).
Att Ports	The number of ports actually attached to this aggregate group.
Sel Ports	The number of ports that could possibly attach to the aggregate group.

A static aggregate is specified:

```
-> show linkagg agg 5

Static Aggregate
  SNMP Id                  : 40000005,
  Aggregate Number         : 5,
  SNMP Descriptor          : Omnichannel Aggregate Number 5 ref 40000005 size 2,
  Name                     : AGG5,
  Admin State              : ENABLED,
  Operational State        : DOWN,
  Aggregate Size           : 2,
  Number of Selected Ports : 0,
  Number of Reserved Ports : 0,
  Number of Attached Ports : 0,
  Primary Port             : NONE
  Port Selection Hash      : Source Destination Ip,
  Wait To Restore Time     : 0 Minutes

-> show linkagg agg 10

Static Loopback Aggregate
  SNMP Id                  : 40000010,
  Aggregate Number         : 20,
  SNMP Descriptor          : Omnichannel Aggregate Number 20 ref 40000020 size 2,
  Name                     : ,
  Admin State              : ENABLED,
  Operational State        : DOWN,
  Aggregate Size           : 2,
  Number of Selected Ports : 0,
  Number of Reserved Ports : 0,
  Number of Attached Ports : 0,
  Primary Port             : NONE,
  Port Selection Hash      : Source Destination Ip,
  Wait To Restore Time     : 0 Minutes
```

output definitions

SNMP Id	The SNMP ID associated with this static aggregate group.
Aggregate Number	The group number.
SNMP Descriptor	The standard MIB name for this static aggregate group.
Name	The name of this static aggregate group. Configured through the **linkagg static agg name** command.
Admin State	The administrative state of this static aggregate group (**ENABLED** or **DISABLED**). Configured through the **linkagg static agg admin-state** command.

output definitions (continued)

Operational State	The operational state of this static aggregate group (**UP** or **DOWN**).
Aggregate Size	The number of links configured for this static aggregate group.
Number of Selected Ports	The number of ports that could possibly attach to this static aggregate group.
Number of Reserved Ports	The total number of ports reserved for use in link aggregation by this static aggregate group. (**Note**: This field is not relevant for static aggregate groups.)
Number of Attached Ports	The number of ports actually attached to this static aggregate group.
Primary Port	The port number of the first port to join this static aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.
Port Selection Hash	The hashing algorithm used to identify a specific traffic flow to hash.
Wait To Restore Time	The amount of time, in minutes, the switch waits to bring up a link aggregate that is attached to other links. Configured through the **linkagg static agg wait-to-restore-time** command.

A dynamic aggregate group is specified:

```
-> show linkagg agg 1-2

Dynamic Aggregate
  SNMP Id                  : 40000002,
  Aggregate Number         : 2,
  SNMP Descriptor          : Dynamic Aggregate Number 2 ref 40000002 size 4,
  Name                     : AGG 2,
  Admin State              : ENABLED,
  Operational State        : DOWN,
  Aggregate Size           : 4,
  Number of Selected Ports : 0,
  Number of Reserved Ports : 0,
  Number of Attached Ports : 0,
  Primary Port             : NONE,
  Port Selection Hash      : Source Destination Ip,
  Wait To Restore Time     : 0 Minutes
LACP
  MACAddress               : [00:1f:cc:00:00:00],
  Actor System Id          : [00:20:da:81:d5:b0],
  Actor System Priority    : 50,
  Actor Admin Key          : 120,
  Actor Oper Key           : 0,
  Partner System Id        : [00:20:da:81:d5:b1],
  Partner System Priority  : 70,
  Partner Admin Key        : 220,
  Partner Oper Key         : 0
```

output definitions

SNMP Id	The SNMP ID associated with this dynamic aggregate group.
Aggregate Number	The group number of this dynamic aggregate group.
SNMP Descriptor	The standard MIB name for this dynamic aggregate group.

output definitions (continued)

Name	The name of this dynamic aggregate group. You can modify this parameter with the **linkagg lacp agg name** command (see page 12-20).
Admin State	The administrative state of this dynamic aggregate group, which can be **ENABLED** or **DISABLED**. You can modify this parameter with the **linkagg lacp agg admin-state** command (see page 12-23).
Operational State	The operational state of this dynamic aggregate group, which can be **UP** or **DOWN**.
Aggregate Size	The number of links configured for this dynamic aggregate group.
Number of Selected Ports	The number of ports available to this dynamic aggregate group.
Number of Reserved Ports	The total number of ports reserved for use in link aggregation by this dynamic aggregate group.
Number of Attached Ports	The number of ports actually attached to this dynamic aggregate group.
Primary Port	The port number of the first port to join this dynamic aggregate group. If the first port to join the aggregate group is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.
Port Selection Hash	The hashing algorithm used to identify a specific traffic flow to hash.
Wait To Restore Time	The amount of time, in minutes, the switch waits to bring up a link aggregate that is attached to other links. Configured through the **linkagg lacp agg wait-to-restore-time** command.
MACAddress	The MAC address associated with the primary port.
Actor System Id	The MAC address of this dynamic aggregate group. You can modify this parameter with the **linkagg lacp agg actor system-id** command (see page 12-28).
Actor System Priority	The priority of this dynamic aggregate group. You can modify this parameter with the **linkagg lacp agg actor system-priority** command (see page 12-26).
Actor Admin Key	The administrative key associated with this dynamic aggregate group. You can modify this parameter with the **linkagg lacp agg actor admin-key** command (see page 12-25).
Actor Oper Key	The operational key associated with this dynamic aggregate group.
Partner System Id	The MAC address of the remote dynamic aggregate group. You can modify this parameter with the **linkagg lacp agg partner system-id** command (see page 12-30).
Partner System Priority	The priority of the remote system to which this dynamic aggregation group is attached. You can modify this parameter with the **linkagg lacp agg partner system-priority** command (see page 12-32).
Partner Admin Key	The administrative key for the remote partner of the dynamic aggregation. You can modify this parameter with the **linkagg lacp agg partner admin-key** command (see page 12-34).
Partner Oper Key	The operational key of the remote system to which the dynamic aggregation group is attached.

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg accounting	Displays statistics for packet frames received and transmitted on link aggregate member ports.
show linkagg counters	Displays statistics for the number of packet frames and errors received and transmitted on link aggregate member ports.

MIB Objects

```
alclnkaggAggTable
   alclnkAggSize
   alclnkaggAggNumber
   alclnkaggAggDescr
   alclnkaggAggName
   alclnkaggAggLacpType
   alclnkaggAggAdminState
   alclnkaggAggOperState
   alclnkaggAggNbrSelectedPorts
   alclnkaggAggNbrAttachedPorts
   alclnkaggPrimaryPortIndex
   alclnkaggAggPortSelectionHash
   alclnkaggAggWTRTimer
   alclnkaggAggMACAddress
   alclnkaggAggActorSystemPriority
   alclnkaggAggActorSystemID
   alclnkaggAggPartnerAdminKey
   alclnkaggAggActorAdminKey
   alclnkaggAggActorOperKey
   alclnkAggLocalRangeOperMin
   alclnkAggLocalRangeOperMax
   alclnkAggLocalRangeConfiguredMin
   alclnkAggLocalRangeConfiguredMax
   alclnkAggPeerRangeOperMin
   alclnkAggPeerRangeOperMax
   alclnkaggAggPartnerSystemID
   alclnkaggAggPartnerSystemPriority
   alclnkaggAggPartnerOperKey
```

show linkagg port

Displays information about link aggregation ports.

show linkagg [agg *agg_id***[-***agg_id2***]] port [***chassis/slot/port***]**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the aggregate group. Use a hyphen to specify a range of IDs (10-20).
chassis	The chassis identifier.
slot/port	The slot and port number of the link aggregation port.

Defaults

By default, all link aggregation ports are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a particular slot or port is specified, the fields displayed depend upon whether the port belongs to a static aggregate group or a dynamic (LACP) aggregate group.
- If only a link aggregate or a range of link aggregates is specified along with the **agg** keyword, the ports and related information for only the specified link aggregate IDs are displayed.
- If multi-chassis feature is activated on the switch, the **show** command displays the link aggregates as MC-Static and MC-Dynamic as shown in the second example.

Examples

```
-> show linkagg port

Slot/Port Aggregate  SNMP Id   Status   Agg  Oper Link Prim
---------+----------+--------+----------+----+----+----+----+----
   2/1    Static        2001  ATTACHED     1  UP   UP   YES
```

Multi-chassis active:

```
-> show linkagg port

Slot/Port Aggregate  SNMP Id   Status   Agg  Oper Link Prim
---------+----------+--------+----------+----+----+----+----+----
   2/1    MC-Static        2001  ATTACHED     1  UP   UP   YES
```

```
-> show linkagg agg 1-5 port
Slot/Port  Aggregate  SNMP Id    Status        Agg Oper Link Prim
---------+-----------+--------+--------------+------+----+----+----+-----
   1/16  Static       2016     CONFIGURED       1    UP   UP   YES
   1/17  Static       2017     CONFIGURED       2    UP   UP   NO
   3/1   Static       3001     CONFIGURED      3     UP   UP   NO
   3/2   Static       3045     CONFIGURED       4    UP   UP   NO
   3/3   Static       3069     CONFIGURED       5    UP   UP   NO
```

Output fields are defined here:

output definitions

Slot/Port	The slot/port associated with the aggregate group.
Aggregate	The type of aggregate group associated with the port, either **Static** or **Dynamic**.
SNMP Id	The SNMP ID associated with the aggregate group.
Status	The current status of the port, which can be **CONFIGURED**, **PENDING**, **SELECTED**, or **RESERVED**.
Agg	The number of the aggregate groups associated with this port.
Oper	The operational status of the port.
Link	The physical link status of the port.
Prim	Specifies if the port is the primary port of the aggregate. The primary port is the lowest numbered port in a link aggregate.

A port that belongs to a static aggregate is specified:

```
-> show linkagg port 4/1

Static Aggregable Port
  SNMP Id                      : 4001,
  Slot/Port                    : 4/1,
  Administrative State         : ENABLED,
  Operational State            : DOWN,
  Port State                   : CONFIGURED,
  Link State                   : DOWN,
  Selected Agg Number          : 2,
  Port position in the aggregate: 0,
  Primary port                 : NONE
```

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this port.
Slot/Port	The slot and port number.
Administrative State	The current administrative state of this port, which can be **ENABLED** or **DISABLED**.
Operational State	The current operational state of the port, which can be **UP** or **DOWN**.
Port State	The current operational state of the port, which can be **CONFIGURED**, **PENDING**, **SELECTED**, or **RESERVED**.

output definitions (continued)

Link State	The current operational state of the link from this port to its remote partner, which can be **UP** or **DOWN**.
Selected Agg Number	The number associated with the static aggregate group to which the port is attached.
Port position in the aggregate	The rank of this port within the static aggregate group.
Primary Port	The port number of the first port to join this static aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.

A port that belongs to a static link aggregate is specified:

```
-> show linkagg agg 1

Static Aggregate
SNMP Id                  : 40000001,
  Aggregate Number       : 1,
  SNMP Descriptor        : Omnichannel Aggregate Number 1 ref 40000001 size 4,
  Name                   : ,
  Admin State            : ENABLED,
  Operational State      : DOWN,
  Aggregate Size         : 4,
  Number of Selected Ports : 0,
  Number of Reserved Ports : 0,
  Number of Attached Ports : 0,
  Primary Port           : NONE
```

A port that belongs to a dynamic aggregate is specified:

```
-> show linkagg port 2/1

Dynamic Aggregable Port
  SNMP Id                      : 2001,
  Slot/Port                    : 2/1,
  Administrative State         : ENABLED,
  Operational State            : DOWN,
  Port State                   : CONFIGURED,
  Link State                   : DOWN,
  Selected Agg Number          : NONE,
  Primary port                 : UNKNOWN,
LACP
  Actor System Priority        : 10,
  Actor System Id              : [00:d0:95:6a:78:3a],
  Actor Admin Key              : 8,
  Actor Oper Key               : 8,
  Partner Admin System Priority : 20,
  Partner Oper System Priority  : 20,
  Partner Admin System Id       : [00:00:00:00:00:00],
  Partner Oper System Id        : [00:00:00:00:00:00],
  Partner Admin Key             : 8,
  Partner Oper Key              : 0,
  Attached Agg Id               : 0,
  Actor Port                    : 7,
  Actor Port Priority           : 15,
  Partner Admin Port            : 0,
```

```
Partner Oper Port             : 0,
Partner Admin Port Priority   : 0,
Partner Oper Port Priority    : 0,
Actor Admin State             : act1.tim1.agg1.syn0.col0.dis0.def1.exp0
Actor Oper State              : act1.tim1.agg1.syn0.col0.dis0.def1.exp0,
Partner Admin State           : act0.tim0.agg1.syn1.col1.dis1.def1.exp0,
Partner Oper State            : act0.tim0.agg1.syn0.col1.dis1.def1.exp0
```

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this port.
Slot/Port	The slot and port number.
Administrative State	The current administrative state of this port, which can be **ENABLED** or **DISABLED**.
Operational State	The current operational state of the port, which can be **UP** or **DOWN**.
Port State	The current operational state of the port, which can be **CONFIGURED**, **PENDING**, **SELECTED**, or **AGGREGATED**.
Link State	The current operational state of the link from this port to its remote partner, which can be **UP** or **DOWN**.
Selected Agg Number	The number associated with the dynamic aggregate group to which the port is attached.
Primary Port	The port number of the first port to join this dynamic aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.
Actor System Priority	The actor system priority of this port. You can modify this parameter with the **linkagg lacp port actor system-priority** command (see page 12-43).
Actor System Id	The actor system ID (i.e., MAC address) of this port. You can modify this parameter with the **linkagg lacp port actor system-id** command (see page 12-41).
Actor Admin Key	The actor administrative key value for this port. You can modify this parameter with the **linkagg lacp port actor admin-key** command (see page 12-36).
Actor Oper Key	The actor operational key associated with this port.
Partner Admin System Priority	The administrative priority of the remote system to which this port is attached. You can modify this parameter with the **linkagg lacp port partner admin system-priority** command (see page 12-52).
Partner Oper System Priority	The operational priority of the remote system to which this port is attached.
Partner Admin System Id	The administrative MAC address associated with the system ID of a remote partner. This value is used along with Partner Admin System Priority, Partner Admin Key, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the **linkagg lacp port partner admin system-id** command (see page 12-48).
Partner Oper System Id	The MAC address that corresponds to the system ID of the remote partner.

output definitions (continued)

Partner Admin Key	The administrative value of the key for the remote partner. This value is used along with Partner Admin System Priority, Partner Admin System, Partner Admin Port, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the **linkagg lacp port partner admin-key** command (see page 12-50).
Partner Oper Key	The current operational value of the key for the protocol partner.
Attached Agg ID	The ID of the aggregate group that the port has attached itself to. A value of zero indicates that the port is not attached to an aggregate group.
Actor Port	The port number locally assigned to this port.
Actor Port Priority	The actor priority value assigned to the port. You can modify this parameter with the **linkagg lacp port actor port priority** command (see page 12-54).
Partner Admin Port	The administrative value of the port number for the protocol partner. This value is used along with Partner Admin System Priority, Partner Admin System ID, Partner Admin Key, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the **linkagg lacp port partner admin-port** command (see page 12-56).
Partner Oper Port	The operational port number assigned to the port by the protocol partner of the port.
Partner Admin Port Priority	The administrative port priority of the protocol partner. This value is used along with Partner Admin System Priority, Partner Admin System ID, and Partner Admin Key to manually configure aggregation. You can modify this parameter with the **linkagg lacp port partner admin port-priority** command (see page 12-57).
Partner Oper Port Priority	The priority value assigned to the this port by the partner.
Actor Admin State	The administrative state of the port. You can modify this parameter with the **linkagg lacp port actor admin-state** command (see page 12-39).
Actor Oper State	The current operational state of the port.
Partner Admin State	The administrative state of the partner port. You can modify this parameter with the **linkagg lacp agg partner admin-state** command (see page 12-45).
Partner Oper State	The current operational state of the partner port.

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static port agg	Configures a slot and port for a static aggregate group.
linkagg lacp port actor admin-key	Configures a slot and port for a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortActorSystem
   alclnkaggAggPortActorSystemPriority
   alclnkaggAggPortActorSystemID
   alclnkaggAggPortActorAdminKey
   alclnkaggAggPortActorOperKey
   alclnkaggAggPortPartnerAdminSystemPriority
   alclnkaggAggPortPartnerOperSystemPriority
   alclnkaggAggPortPartnerAdminSystemID
   alclnkaggAggPortPartnerOperSystemID
   alclnkaggAggPortPartnerAdminKey
   alclnkaggAggPortPartnerOperKey
   alclnkaggAggPortSelectedAggID
   alclnkaggAggPortAttachedAggID
   alclnkaggAggPortActorPort
   alclnkaggAggPortActorPortPriority
   alclnkaggAggPortPartnerAdminPort
   alclnkaggAggPortPartnerOperPort
   alclnkaggAggPortPartnerAdminPortPriority
   alclnkaggAggPortPartnerOperPortPriority
   alclnkaggAggPortActorAdminState
   alclnkaggAggPortActorOperState
   alclnkaggAggPortPartnerAdminState
   alclnkaggAggPortPartnerOperState
```

show linkagg accounting

Displays statistics collected for packets transmitted and received on link aggregate ports.

show linkagg accounting

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Statistics are displayed for all link aggregate IDs configured on the switch.
- Statistics are collected for undersized and oversized packets, packets of a certain size, and Jabber frames.

Examples

```
-> show linkagg accounting

Link Agg 10
rx undersize packets    = 0
tx undersize packets    = 0
rx oversize packets     = 0
tx oversize packets     = 0
rx packets 64           = 3073753
rx packets 65_127       = 678698
rx packets 128_255      = 21616
rx packets 256_511      = 21062
rx packets 512_1023     = 2
rx packets 1024_1518    = 84
rx packets 1519_4095    = 0
rx packets 4096_9216    = 0
rx jabber frames         = 0
```

Release History

Release 8.3.1; command introduced.

Related Commands

show linkagg counters	Displays statistics collected for the type and number of packets transmitted and received on link aggregate ports.
show linkagg traffic	Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.
clear linkagg-statistics	Clears statistics for all link aggregates or for specific aggregate IDs.

MIB Objects

```
lnkaggAggIdAccountTable
   alcRxUndersize
   alcTxUndersize
   alcRxOversize
   alcTxOversize
   alcRxPackets64
   alcRxPackets127
   alcRxPackets255
   alcRxPackets511
   alcRxPackets1023
   alcRxPackets1518
   alcRxPackets4095
   alcRxPackets9216
   alcRxJabberFrames
```

show linkagg counters

Displays statistics collected for the type and number of packet frames transmitted and received on link aggregate ports.

show linkagg counters [errors]

Syntax Definitions

errors	Display the number of errors received on the link aggregate member ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Statistics are displayed (in bytes or frame count) for all link aggregate IDs configured on the switch.
- Error statistics include the number of alignment, frame check (FCS), received, and transmitted errors.

Examples

```
-> show linkagg counters

Link Agg 10
InOctets                = 54367578586897979
OutOctets               = 5.78E19
InUcastPkts             = 55654265276
OutUcastPkts            = 5.78E20
InMcastPkts             = 58767867868768777
OutMcastPkts            = 5465758756856
InBcastPkts             = 576567567567567576
OutBcastPkts            = 786876
InPause frames          = 567798768768767
OutPause frames         = 786876

-> show linkagg counters errors

Link Agg 10
Alignments Errors       = 6.45E13
FCS Errors              = 7.65E12
IfInErrors              = 6435346
IfOutErrors             = 5543
```

Release History

Release 8.3.1; command introduced.

Related Commands

show linkagg accounting	Displays statistics collected for packets transmitted and received on link aggregate ports.
show linkagg traffic	Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.
clear linkagg-statistics	Clears statistics for all link aggregates or for specific aggregate IDs.

MIB Objects

```
alclnkaggAggIdCounterTable
   alcInOctets
   alcOutOctets
   alcInUcastPkts
   alcOutUcastPkts
   alcInMcastPkts
   alcOutMcastPkts
   alcInBcastPkts
   alcOutBcastPkts
   alcInPauseFrames
   alcOutPauseFrames
```

show linkagg traffic

Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.

show linkagg traffic

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Statistics are displayed for all link aggregate IDs configured on the switch.

Examples

```
-> show linkagg traffic
         Input      Input           Output     Output
Agg      Packets    Bytes           Packets    Bytes
--------+----------+---------------+----------+---------------
10       322        20624           5125       347216
20       456        30620           6133       397764
```

Release History

Release 8.3.1; command introduced.

Related Commands

show linkagg accounting	Displays statistics collected for packets transmitted and received on link aggregate ports.
show linkagg counters	Displays statistics collected for the type and number of packets transmitted and received on link aggregate ports.
clear linkagg-statistics	Clears statistics for all link aggregates or for specific aggregate IDs.

MIB Objects

```
alclnkaggAggIdTrafficTable
   alcInputPackets
   alcInputBytes
   alcOutputPackets
   alcOutputBytes
```

clear linkagg-statistics

Clears statistics for all link aggregates or for a specific aggregate ID or range of IDs.

clear linkagg-statistics [agg *agg_id***[**-*agg_id2***]]**

Syntax Definitions

*agg_id***[**-*agg_id2***]**	The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, statistics are cleared for all link aggregates.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command sets all statistic counters to zero.

Examples

```
-> clear linkagg-statistics
-> clear linkagg-statistics agg 10
-> clear linkagg-statistics agg 11-15
```

Release History

Release 8.3.1; command introduced.

Related Commands

show linkagg accounting	Displays statistics collected for packets transmitted and received on link aggregate ports.
show linkagg counters	Displays statistics collected for the type and number of packets transmitted and received on link aggregate ports.
show linkagg traffic	Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.

MIB Objects

```
alclnkaggAggPortStatsTable
   alclnkaggAggPortStatsLACPDUsRx
   alclnkaggAggPortStatsMarkerPDUsRx
   alclnkaggAggPortStatsMarkerResponsePDUsRx
   alclnkaggAggPortStatsUnknownRx
   alclnkaggAggPortStatsIllegalRx
   alclnkaggAggPortStatsLACPDUsTx
   alclnkaggAggPortStatsMarkerPDUsTx
   alclnkaggAggPortStatsMarkerResponsePDUsTx
```

show linkagg range

Displays information about the configured or operational link aggregate range identifiers for standard and MC-LAG link aggregates.

show linkagg range [operation | config]

Syntax Definitions

operation	Displays the operational ranges.
config	Displays the configured ranges.

Defaults

By default, both the operational and configured ranges are shown.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **operation** parameter to display only the operational link aggregate identifiers.
- Use the **config** parameter to display only the configured link aggregate identifiers.
- A chassis reboot is required for the configured values to become operational.

Examples

```
-> show linkagg range
                      Operational            Configured
                      Min       Max          Min     Max
--------------------+--------+--------+-------------+-------+
Local                   0       127             0         0
Peer                    0       127             0         0
Multi-Chassis           0       127             0       127
```

output definitions

Operational Min/Max	The currently operational ranges.
Configured Min/Max	The currently configured ranges.
Local	The local link aggregate identifiers.
Peer	The peer link aggregate identifiers.
Multi-Chassis	The multi-chassis link aggregate identifiers.

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg range	Configures the standard and MC-LAG aggregate identifier ranges.

MIB Objects

```
alclnkaggAggConfig
   alclnkAggLocalRangeOperMin
   alclnkAggLocalRangeOperMax
   alclnkAggLocalRangeConfiguredMin
   alclnkAggLocalRangeConfiguredMax
   alclnkAggPeerRangeOperMin
   alclnkAggPeerRangeOperMax
   alclnkAggPeerRangeConfiguredMin
   alclnkAggPeerRangeConfiguredMax
   alclnkAggMcLagRangeOperMin
   alclnkAggMcLagRangeOperMax
   alclnkAggMcLagRangeConfiguredMin
   alclnkAggMcLagRangeConfiguredMax
```

13 Virtual Chassis Commands

A Virtual Chassis is a group of switches managed through a single management IP address and that behave as a single bridge or router. It provides both node level and link level redundancy for devices connecting to the aggregation layer via dual-homed standard 802.3ad link aggregation mechanisms. The use of Virtual Chassis provides node level redundancy without the need to use redundancy protocols such as STP and VRRP between the edge and the aggregation/core layer.

MIB information for the Virtual Chassis commands is as follows:

Filename: ALCATEL-IND1-VIRTUAL-CHASSIS-MIB.mib
Module: alcatelIND1VirtualChassisMIB

Filename: ALCATEL-IND1-VC-SPLIT-PROTECTION-MIB.mib
Module: alaVCSPMIB

A summary of available commands is listed here:

Virtual Chassis Commands	**virtual-chassis configured-chassis-id** **virtual-chassis chassis-group** **virtual-chassis configured-chassis-priority** **virtual-chassis configured-control-vlan** **virtual-chassis configured-hello-interval** **virtual-chassis vf-link create** **virtual-chassis vf-link member-port** **virtual-chassis vf-link default-vlan** **virtual-chassis hello-interval** **virtual-chassis shutdown** **virtual-chassis vf-link-mode** **virtual-chassis auto-vf-link-port** **vc-takeover** **convert configuration** **show virtual-chassis topology** **show virtual-chassis consistency** **show virtual-chassis vf-link** **show virtual-chassis auto-vf-link-port** **show virtual-chassis chassis-reset-list** **show virtual-chassis slot-reset-list** **show virtual-chassis consistency** **show virtual-chassis neighbors** **show configuration vcm-snapshot chassis-id**
Virtual Chassis Split Protection Commands	**virtual-chassis split-protection admin-state** **virtual-chassis split-protection linkagg** **virtual-chassis split-protection guard-timer** **virtual-chassis split-protection helper admin-state** **virtual-chassis split-protection helper linkagg** **show virtual-chassis split-protection status** **show virtual-chassis split-protection vc-units** **show virtual-chassis split-protection helper status**

virtual-chassis configured-chassis-id

Assigns a globally unique chassis identifier to the switch and enables the switch to operate in virtual-chassis mode.

virtual-chassis [chassis-id *oper_chassis***] configured-chassis-id** *config_chassis*

no virtual-chassis [chassis-id *oper_chassis***] configured-chassis-id** *config_chassis*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
config_chassis	The configured/next chassis ID number.

Defaults

parameter	default
oper_chassis	0 (standalone mode; no virtual chassis operation is allowed)

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to change the chassis ID back to “0” (the default). When the chassis ID is set to “0”, the switch operates in standalone mode and all virtual chassis related configuration commands are no longer active for the switch.
- The operational chassis identifier parameter is only optional when the switch is running in standalone mode or at start up time, within the *vcsetup.cfg*, when the switch is coming up in virtual chassis mode. The same restrictions apply to the no form of the command.
- The operational chassis identifier is a mandatory parameter whenever the system is running in virtual chassis mode. This prevents modifying the chassis identifier of all switches at the same time and causing a duplicate chassis identifier.
- Two switches that have the same chassis identifier are not allowed to operate in virtual chassis mode. If a duplicate chassis identifier is detected one of the switches will be in an inconsistent role and its status will be set to Duplicate-Chassis-ID.
- The configured chassis identifier will only take effect after the next reboot of the target chassis.
- Virtual chassis is only supported between two switches of the same type. For example, virtual chassis is not supported between an OmniSwitch 6860 and an OmniSwitch 6900.
- The no form of this command can only be used if there are no VFLs configured on the switch.
- Snapshots produced through the **show configuration vcm-snapshot**, **show configuration snapshot virtual chassis** or **write memory** commands always include the operational chassis identifier.

Examples

```
-> virtual-chassis configured-chassis-id 1 //Standalone mode
-> virtual-chassis chassis-id 0 configured-chassis-id 1
-> no virtual-chassis chassis-id 0 configured-chassis-id
-> no virtual-chassis configured-chassis-id
```

Release History

Release 7.3.1; command introduced.

Related Commands

vc-takeover	Converts an existing standalone configuration to a virtual chassis configuration.
show virtual-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.
show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasId
   virtualChassisConfigChassisId
```

virtual-chassis chassis-group

Assigns a globally unique chassis group identifier to a chassis. Each peer switch in a virtual chassis domain must use the same group ID number. The group ID number uniquely identifies switches operating in the same virtual chassis.

virtual-chassis [chassis-id *oper_chassis***] chassis-group** *group*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
group	Virtual chassis group identifier (0-255), which is used to identify a group of chassis belonging to the same virtual chassis.

Defaults

parameter	default
group	Derived from last byte of Master chassis MAC address

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Each virtual chassis domain must use a different group ID number to differentiate the domain within the network environment.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches is running in virtual chassis mode the chassis group can only be configured with exactly the same value as the master chassis when the configuration applies to a single and specific switch.
- When a set of switches is running in virtual chassis mode the chassis group can be configured with any value within the valid range as long as the configuration applies to all switches at the same time.
- It is strongly recommended that the same chassis group value is set for all switches that will participate on the same virtual chassis group. Failure to adhere to this recommendation followed by a system reset will prevent the switches whose values are different from joining the same virtual chassis group.
- When determining the chassis group ID the last byte of the Master chassis MAC address is used. For example, if the Master's MAC address is xx:xx:xx:xx:xx:7e, the chassis group will be 126 (equivalent to hex 7e).

Examples

```
-> virtual-chassis chassis-id 1 chassis-group 10
-> virtual-chassis chassid-id 0 chassis-group 10
-> virtual-chassis chassis-group 10 // All switches
```

Release History

Release 7.3.1; command introduced.
Release 7.3.4; Chassis group ID based on Master MAC address introduced.

Related Commands

vc-takeover	Converts an existing standalone configuration to a virtual chassis configuration
show virtual-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.
show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasID
   virtualChassisGroup
```

virtual-chassis configured-chassis-priority

Sets the configured chassis priority for a chassis specified by its operational chassis identifier.

virtual-chassis [chassis-id *oper_chassis***] configured-chassis-priority** *priority*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
priority	Configured chassis priority (0-255) which defines the user preference above all other election criteria, for the target chassis to become the master of the virtual chassis.

Defaults

parameter	default
priority	OS6900-Q32 - 120 All others - 100

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The greatest configured-chassis-priority will become the Master chassis. Without setting this value the smallest chassis identifier becomes the key parameter used to determine which switch will become the Master.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- The configured chassis priority will only take effect after the next reboot of the target switch.

Examples

Standalone mode:

```
-> virtual-chassis chassis-priority 50
-> virtual-chassis chassis-id 0 chassis-priority 50
```

All switches:

```
-> virtual-chassis configured-chassis-priority 50
-> virtual-chassis chassid-id 0 configured-chassis-priority 50
```

Chassis 2 only:

```
-> virtual-chassis chassis-id 2 configured-chassis-priority 75 //Chassis 2 only
```

Release History

Release 7.3.1.R01; command introduced.

Related Commands

vc-takeover	Converts an existing standalone configuration to a virtual chassis configuration.
show virtual-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.
show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasID
   virtualChassisConfigPriority
```

virtual-chassis configured-control-vlan

Sets the configured control VLAN for a chassis specified by its operational chassis identifier.

virtual-chassis [chassis-id *oper_chassis***] configured-control-vlan** *vlan*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
vlan	Configured/next virtual chassis control VLAN (2-4094), which is used for all internal control communication between switches over the VFL.

Defaults

parameter	default
vlan	4094

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This configured control VLAN will only take effect after the next reboot of the target switch.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches in running in virtual chassis mode, the configured control VLAN can only be configured with exactly the same value as the master chassis when the configuration applies to a single and specific switch.
- When a set of switches in running in virtual chassis mode, the configured control VLAN can be configured with any value within the valid range as long as the configuration applies to all switches at the same time.
- It is strongly recommended that the value is for all switches that will participate in the same virtual chassis topology.

Examples

Standalone mode:

```
-> virtual-chassis configured-control-vlan 10
-> virtual-chassis chassis-id 0 configured-control-vlan 10
```

All switches:

```
-> virtual-chassis configured-control-vlan 10
-> virtual-chassis chassis-id 0 configured-control-vlan 10
```

Release History

Release 7.3.1; command introduced.

Related Commands

vc-takeover	Converts an existing standalone configuration to a virtual chassis configuration.
show virtual-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.
show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasID
   virtualChassisConfigControlVlan
```

virtual-chassis configured-hello-interval

Sets the virtual chassis configured hello interval parameter on the switch. Hello packets are sent periodically on the virtual fabric link (VFL) interfaces to establish a relationship and bidirectional communication between virtual chassis switches. The hello interval value determines how often these packets are sent.

virtual-chassis [chassis-id *oper_chassis***] configured-hello-interval** *hello*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
hello	Configured/next virtual chassis hello interval in seconds (1-10), which defines how frequently the keep-alives related to the virtual chassis hello protocol are exchanged over the VFL links.

Defaults

parameter	default
hello	5

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configured value will only take effect after the next reboot of the target switch.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches is running in virtual chassis mode, the configured hello interval can only be configured with exactly the same value as the master chassis when the configuration applies to a single and specific switch.
- When a set of switches is running in virtual chassis mode, the configured hello interval can be configured with any value within the valid range as long as the configuration applies to all switches at the same time.
- The hello timeout is a fixed value and defined as 120 seconds. This is the minimum time interval that a switch will wait without receiving any hello packets from a peer switch before declaring that the adjacency towards that switch was lost.
- It is strongly recommended that the hello interval be the same for all switches that will participate in the same virtual chassis topology.

Examples

Standalone mode:

```
-> virtual-chassis configured-hello-interval 10
-> virtual-chassis chassis-id 0 configured-hello-interval 10
```

All switches:

```
-> virtual-chassis configured-hello-interval 10
-> virtual-chassis chassis-id 0 configured-hello-interval 10
```

Release History

Release 7.3.1; command introduced.
Release 7.3.3; command deprecated.

Related Commands

vc-takeover	Converts an existing standalone configuration to a virtual chassis configuration.
show virtual-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.
show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasID
   virtualChassisConfigHelloInterval
```

virtual-chassis vf-link create

Configures a virtual fabric link (VFL) between two peer switches. A VFL is required to enable the virtual chassis operation between the two switches.

virtual-chassis [chassis-id *oper_chassis***] vf-link** *vfl_id* **create**

no virtual-chassis [chassis-id *oper_chassis***] vf-link** *vfl_id*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
vfl_id	The VFL link identifier (0).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Although a virtual fabric link can be configured while the switch is running either in standalone or virtual chassis mode, a VFL can only become operational when the chassis operates in virtual chassis mode.
- Use the no form of this command to remove the VFL configuration from the switch.
- Although the switch supports runtime configuration of the VFL and its member ports, configuring the VFL at the same time as the chassis identifier is configured and before rebooting the switch is recommended.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- This command is valid only when the VFL mode is set to static.

Examples

```
-> virtual-chassis vf-link 0 create
-> virtual-chassis chassis-id 0 vf-link 0 create
-> no virtual-chassis vf-link 0
-> no virtual-chassis chassis-id 0 vf-link 0

-> virtual-chassis chassis-id 1 vf-link 0 create
-> virtual-chassis chassis-id 2 vf-link 0 create
-> no virtual-chassis chassis-id 1 vf-link 0
-> no virtual-chassis chassis-id 2 vf-link 0
```

Release History

Release 7.3.1; command introduced.

Related Commands

vc-takeover	Converts an existing standalone configuration to a virtual chassis configuration.
show virtual-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.
show virtual-chassis vf-link	Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

MIB Objects

```
virtualChassisLinkTable
   virtualChassisOperChasID
   virtualChassisLinkID
   virtualChassisVflRowStatus
```

virtual-chassis vf-link member-port

Adds member ports to a given virtual fabric link (VFL).

virtual-chassis [chassis-id *oper_chassis***] vf-link** *vfl_id* **member-port [***oper_chassis/***]***slot/port*

no virtual-chassis [chassis-id *oper_chassis***] vf-link** *vfl_id* **member-port [***oper_chassis/***]***slot/port*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
vfl_id	The VFL link identifier (0).
oper_chassis/slot/port	The operational chassis identifier, slot, and port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Although virtual-fabric link (VFL) member ports can be configured while the switch is running either in standalone or virtual chassis mode, a configured virtual-fabric link (VFL) member port can only become operational when the chassis operates in virtual chassis mode.
- Use the no form of this command to remove a member port from the virtual-fabric link (VFL).
- When a switch is running in virtual chassis mode, a virtual-fabric link member port must be fully specified including *oper_chassis/slot/port*.
- Although the switch supports runtime configuration of the virtual-fabric link (VFL) and its member ports, configuring the virtual-fabric link (VFL) at the same time as the chassis identifier is configured and before rebooting the switch is recommended.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches in running in virtual chassis mode, a virtual-fabric link (VFL) member ports can only be created or removed exactly in one switch at a time. In other words, we are not allowed to create or remove a virtual chassis link member port with a system operating in virtual chassis mode if no operational chassis identifier is provided or if the value zero is specified.
- A maximum of 16 member ports can be added or assigned to each virtual-fabric link (VFL).
- All virtual-fabric link (VFL) member ports must operate at the same speed.
- Only interfaces that operate at 10 Gbps or 40 Gbps can be added or assigned to a virtual-fabric link. (**Note**: 10GBaseT ports cannot be assigned to a VFL).
- Only interfaces operating in full-duplex mode can be added or assigned to a virtual-fabric link.

- It is recommended to configure virtual-fabric link (VFL) member ports across multiple network interface modules (NI) for resilience reasons.
- Virtual-fabric link (VFL) member ports can only be configured on interfaces that are fixed ports, network ports or priority flow control enabled ports. For instance, interfaces configured as Q-tag ports or ERP ports cannot be configured as virtual-fabric link member ports.
- When a switch is running in virtual chassis mode, the interface related to the last active virtual-fabric link member port cannot be administratively disabled.
- When a switch is running in virtual chassis mode, the last active virtual-fabric link member port cannot be deleted using the no form of the present command.
- When a switch is running in virtual chassis mode, the network interface module (NI) that hosts the last active virtual-fabric link member port cannot be administratively reset or powered off.
- This command is valid only when the VFL mode is set to static.

Examples

```
-> virtual-chassis chassis-id 0 vf-link 1 member-port 0/1/1
-> virtual-chassis chassis-id 0 vf-link 1 member-port 0/2/1
-> virtual-chassis chassis-id 1 vf-link 1 member-port 1/1/1
-> virtual-chassis chassis-id 1 vf-link 1 member-port 1/2/1
-> no virtual-chassis chassis-id 0 vf-link 1 member-port 0/1/1
-> no virtual-chassis chassis-id 0 vf-link 1 member-port 0/2/1
-> no virtual-chassis chassis-id 1 vf-link 1 member-port 1/1/1
-> no virtual-chassis chassis-id 1 vf-link 1 member-port 1/2/1
```

Release History

Release 7.3.1; command introduced.

Related Commands

show virtual-chassis consistency	Displays information about the virtual fabric link on the switch.
show virtual-chassis chassis-reset-list	Displays detailed information about the virtual fabric link member ports on the switch.
show virtual-chassis vf-link	Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

MIB Objects

```
virtualChassisLinkTable
   virtualChassisOperChasID
   virtualChassisLinkId
   virtualChassisVflMemberPortIfindex
   virtualChassisVflMemberPortRowStatus
```

virtual-chassis vf-link default-vlan

Configures the default VLAN for the virtual fabric link (VFL).

virtual-chassis [chassis-id *oper_chassis***] vf-link** *vfl_id* **default-vlan** *vlan*

no virtual-chassis [chassis-id *oper_chassis***] vf-link** *vfl_id* **default-vlan**

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
vfl_id	The VFL link identifier (0).
vlan	The default VLAN (1-4094) for the specified VFL.

Defaults

parameter	default
vlan	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This configured VLAN will become the default untagged VLAN for the VFL.
- Although the switch supports runtime configuration of the virtual-fabric link (VFL) and its member ports, configuring the virtual-fabric link (VFL) at the same time as the chassis identifier is configured and before rebooting the switch is recommended.
- Use the **no** form of this command to set the default VLAN back to 1.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches is running in virtual chassis mode, a virtual-fabric link (VFL) default VLAN can only be configured exactly in one switch at a time. In other words, we are not allowed to configured the virtual chassis link default VLAN with a system operating in virtual chassis mode if no operational chassis identifier is provided or if the value zero is specified.
- It is strongly recommended that the user set the same value of default VLAN for all virtual-fabric links on all switches that will participate on the same virtual chassis topology. Failure to adhere to this recommendation may cause end to end connectivity problems in the network.

Examples

Standalone mode:

```
-> virtual-chassis vf-link 0 default-vlan 5
-> virtual-chassis chassis-id 0 vf-link 0 default-vlan 5
-> no virtual-chassis vf-link 0 default-vlan
-> no virtual-chassis chassis-id 0 vf-link 0 default-vlan
```

Chassis 1:

```
-> virtual-chassis chassis-id 1 vf-link 0 default-vlan 5
-> no virtual-chassis chassis-id 1 vf-link 0 default-vlan
```

Release History

Release 7.3.1; command introduced.
Release 7.3.4; command deprecated.

Related Commands

show virtual-chassis vf-link	Displays information about the virtual fabric link on the switch.

MIB Objects

```
virtualChassisLinkTable
   virtualChassisOperChasID
   virtualChassisLinkID
   virtualChassisLinkOperDefaultVlan
```

virtual-chassis hello-interval

Sets the virtual chassis configured hello interval parameter on the chassis. Hello packets are sent periodically on the virtual fabric link (VFL) interfaces to establish a relationship and bidirectional communication between virtual chassis switches. The hello interval value determines how often these packets are sent.

virtual-chassis [chassis-id *oper_chassis***] hello-interval** *hello*

Syntax Definitions

oper_chassis	The operational/current chassis ID number
hello	The operational/current virtual chassis hello interval in seconds (1–2000), which defines how frequently the keep-alives related to the virtual chassis hello protocol are exchanged over the VFL links.

Defaults

parameter	default
hello	2

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches is running in virtual chassis mode, the configured hello interval can only be configured with exactly the same value as the master chassis when the configuration applies to a single and specific switch.
- When a set of switches is running in virtual chassis mode, the hello interval can be configured with any value within the valid range as long as the configuration applies to all switches at the same time.
- It is strongly recommended that the hello interval be the same for all switches that will participate in the same virtual chassis topology.

Examples

Standalone mode:

```
-> virtual-chassis hello-interval 10
-> virtual-chassis chassis-id 0 hello-interval 10
```

Virtual chassis mode:

```
-> virtual-chassis hello-interval 10 //All chassis
-> virtual-chassis chassis-id 2 configured-hello-interval 10 //Chassis 2 only
```

Release History

Release 7.3.3; command introduced.

Related Commands

vc-takeover	Converts an existing standalone configuration to a virtual chassis configuration.
show virtual-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.
show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasID
   virtualChassisOperHelloInterval
```

virtual-chassis shutdown

Disables all front-panel port including the user ports and all the VFL member ports on a chassis isolating the chassis from the rest of the virtual chassis topology.

virtual-chassis shutdown [chassis-id *oper_chassis***]**

Syntax Definitions

oper_chassis	The operational/current chassis ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command will disable all front panel ports, including the user ports and all virtual-fabric link (VFL) member ports on the specified switch.
- After running this command remote access to the target switch is only possible through the local EMP port on that switch.
- The target switch must be reloaded to bring its ports back to an operational state.
- This command is only functional when executed through the master chassis of a system operating in virtual chassis mode.
- After the shutdown command is executed, the target switch assumes the role of master and remains isolated from all other switches in the virtual chassis topology.

Examples

```
-> virtual-chassis shutdown chassis-id 2
```

Release History

Release 7.3.1; command introduced.

Related Commands

show virtual-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

N/A

virtual-chassis vf-link-mode

Configures the Virtual Chassis mode. Virtual Chassis mode determines whether the VFLs are created automatically or statically.

virtual-chassis vf-link-mode {static | auto}

Syntax Definitions

N/A

Defaults

parameter	default
vf-link-mode	**auto** (if no vcsetup.cfg file exists).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

- If the chassis boots without a **vcsetup.cfg** file the mode defaults to auto.
- If the chassis boots with a **vcsetup.cfg** file and the 'virtual-chassis vf-link-mode' CLI does not exist, the mode will be set to static. Otherwise, the mode will be set as configured in the **vcsetup.cfg** file.
- Changing the mode is only allowed for all chassis or the local chassis. Specific chassis configuration is not allowed.

Examples

```
-> virtual-chassis vf-link-mode auto
-> virtual-chassis vf-link-mode static
```

Release History

Release 7.3.4; command introduced.

Related Commands

show virtual-chassis vf-link	Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasID
   virtualChassisVflMode
```

virtual-chassis auto-vf-link-port

Configures the port to be an automatic VFL port.

[no] virtual-chassis auto-vf-link-port *chassis/slot/port*

Syntax Definitions

chassis/slot/port	The operational chassis ID, slot, and port.

Defaults

chassis type	default
OS6900-X/T Models	The last 5 ports including ports on expansion slots.
OS6900-Q32	The last 5 ports that have a transceiver or 40G-to-10G splitter cable plugged in.
OS6900-X72	The last 5 ports (50-54). A port that has a 40G-to-10G splitter cable will be counted as four ports.
OS6900-V72/C32	The last 5 ports. A port that has a splitter cable will be counted as four ports.
OS6860 Models	Dedicated VFL ports.
OS6865 Models	None.
OS6560 Models	OS6560-(P)24X4 - Ports 29-30. OS6560-(P)48X4 - Ports 53-54. Dedicated VFL ports. (all other models).
OS9900	None. Supports static VFL ports only.
OS6465	OS6465-P6/P12 - None. OS6465-P28 - Ports 27/28.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

- This command is allowed only if VFL mode is auto.
- Refer to the defaults table above for information on which ports are default automatic VFL ports.
- Transceiver does not have to be present for port to be eligible as a default port.

Examples

```
-> virtual-chassis auto-vf-link-port 1/1/1
-> no virtual-chassis auto-vf-link-port 1/1/1
```

Release History

Release 7.3.4; command introduced.

Related Commands

show virtual-chassis auto-vf-link-port	Displays a summary of the auto VFL ports.

MIB Objects

```
virtualChassisAutoVflPortTable
   virtualChassisAutoVflPortIfindex
   virtualChassisAutoVflPortRowStatus
```

vc-takeover

This command causes a reload of the master chassis from the running configuration in a virtual chassis environment.

vc-takeover

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- For a dual-CMM Master chassis configuration, this command triggers a local CMM takeover on the Master if both the primary and secondary CMMs are up. This will cause the secondary CMM to become the primary CMM and the NIs will remain up. The original Master chassis will remain the Master and the Slave chassis will remain the Slave.
- For a single-CMM Master chassis configuration, this command will reboot the entire Master chassis including the NIs and result in the Slave chassis becoming the Master.

Examples

```
-> vc-takeover
WARNING - Working Changes Will Be Lost, Confirm VC takeover (Y/N) :
```

Release History

Release 7.3.2; command introduced.

Related Commands

reload from	Reloads the master or slave chassis from the specified directory.

MIB Objects

N/A

convert configuration

Converts an existing standalone configuration to a virtual chassis configuration.

convert configuration to *dir* **[reload]**

Syntax Definitions

dir	The name of the directory to store the virtual chassis configuration.
reload	Reloads the switch after converting the configuration.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command will automatically create the new configuration files *vcsetup.cfg* and *vcboot.cfg* within the specified directory. The *vcsetup.cfg* file contains the virtual chassis manager configuration, which is specific to each individual switch. The contents of the *vcsetup.cfg* files are unique to each switch and distinct between switches. The *vcboot.cfg* file contains the generic application configuration, which is global to the entire virtual chassis topology. As a result, the *vcboot.cfg* files should have the same contents between distinct switches.
- This command will automatically copy the image files of the current running directory into the specified dir directory.
- This command is only accepted in standalone mode after a valid chassis identifier (1-6) has been configured on the switch. The command is rejected when executed in a switch already running in virtual chassis mode.
- The directory will be automatically created if it does not exist.
- The current standalone configuration files (e.g. boot.cfg) that may exist in the directory will remain intact.When the switches come up in virtual chassis mode following a conversion using this command, the *vcboot.cfg* files present on distinct switches may be different. However, the *vcboot.cfg* files must be the same on all switches running in virtual chassis mode. As a result, the *vcboot.cfg* file of the master will overwrite the *vcboot.cfg* file on the slave chassis and the slave will automatically reboot.

Examples

```
-> convert configuration to vc_dir
```

Release History

Release 7.3.1; command introduced.

Related Commands

show configuration snapshot	Displays the configured and operational parameters related to the virtual chassis feature on the switch.

MIB Objects

N/A

show virtual-chassis topology

This command is used to provide a detailed status of the virtual chassis topology.

show virtual-chassis [chassis-id {*oper_chassis*}**] topology**

Syntax Definitions

oper_chassis	The operational/current chassis ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command can be executed on any CMM within any switch of the system.
- When no operational chassis identifier is specified the command will show data related to the entire virtual chassis system.
- A chassis-id of 100 or 101 is used to indicate a duplicate chassis-id.

Examples

```
-> show virtual-chassis topology
Legend: Licenses - A: Advanced; B: Data Center
                                        Config
 Chas  Role         Status              Chas ID  Pri   Group  MAC-Address
-----+------------+-------------------+--------+-----+------+-----------------
1     Master       Running             1        100   1      e8:e7:32:00:2a:55
2     Slave        Running             2        100   1      e8:e7:32:07:9f:e1

-> show virtual-chassis chassis-id 2 topology
Oper-Chassis-ID                 : 2,
Config-Chassis-ID               : 2,
Chassis-Role                    : Master,
Previous-Chassis-Role           : Master,
Chassis-Status                  : Running,
Chassis-Group                   : 1,
Chassis-MAC                     : e8:e7:32:00:2a:55,
Up-Time                         : 0 days 0 hours 22 minutes and 7 seconds,
Designated-NI                   : 1,
Primary-CMM                     : CMM-A,
Secondary-CMM                   : Unknown,
Chassis-Type                    : OS6900,
Licence                         : AB,
Hello-Interval                  : 10,
Oper-Chassis-Priority           : 100,
Config-Chassis-Priority         : 100,
Oper-Control-VLAN               : 4093,
```

```
Config-Control-VLAN             : 4093,
VFLink Mode                     : static,
Number-Of-Neighbors             : 5,
Number-Of-Direct-Neighbors      : 3

Chassis-ID  Is-Direct  Shortest-Path
------------+----------+--------------------
     1         Yes        2/0->1/4
     3         Yes        2/2->3/0
     4         No         2/2->3/0, 3/3->4/2
     5         Yes        2/1->5/1
     6         No         2/0->1/4, 1/0->6/0
```

output definitions

Oper-Chassis-ID (Chas)	Operational/current virtual chassis chassis identifier.
Config Chas ID	The configured/next chassis identifier for the switch specified by operational chassis identifier.
Chassis-Role (Role)	Chassis Role **Unassigned**: Role undefined as election has not completed yet. **Master**: Chassis is central point of management and control. **Slave**: Chassis is an active or functional participant of the virtual chassis topology, but it is not the main entry point for management and control purposes. **Inconsis**: Chassis is not an active or functional participant of the virtual chassis topology due to some inconsistent parameter, which does not match the match the master chassis' settings. **Startup-Err**: Chassis is in start up error mode because it was unable to come up in virtual chassis mode. When a chassis assumes the Startup-Err role, its chassis status will be equal to either Invalid-Chassis-Id or Invalid-License, which are described later in this section.
Previous-Chassis-Role	Previous chassis role before the last transition.

output definitions

Chassis-Status (Status)	Chassis Status **Init**: Status undefined as the chassis has not completed its initialization. **Running**: The chassis is fully operational. **Invalid-Chassis-Id**: The chassis is not operational in virtual chassis mode because no valid chassis identifier has been found in the configuration. Typically this means that the vcsetup.cfg file is corrupted, empty or contains an invalid (e.g. out of range) chassis ID identifier. **Invalid-License**: The chassis is not operational in virtual chassis mode because no valid advanced license has been found. **Hello-Down**: The chassis is isolated from the rest of the virtual chassis topology participants because hello packets have not been received for a period of time greater than the hello timeout. **Duplicate-Chassis**: This chassis is not fully operational because its operational chassis identifier matches the chassis ID of another chassis within the virtual chassis topology. As a result, a new operational chassis identifier from the range (101-102) will be allocated to this chassis. **Mis-Image**: The chassis is not fully operational because its image versions are not consistent with the master chassis' images. In other words, the image version are not compatible and some of the software components running on this chassis are unable to interface with the software operating in the master chassis. **Mis-Chassis-Type**: The chassis is not fully operational because its chassis type (i.e. OS6900, OS6860) is not consistent with the master chassis' type. Different chassis types cannot be mixed in the same virtual chassis topology. **Mis-Hello-Interval**: The chassis is not fully operational because its operational hello interval is not consistent with the master chassis' operational hello interval. **Mis-Control-Vlan**: The chassis is not fully operational because its operational control VLAN is not consistent with the master chassis' operational control VLAN. **Mis-Chassis-Group**: The chassis is not fully operational because its chassis group does not match the master chassis' chassis group and the chassis is connected directly or indirectly to the master chassis through virtual-fabric links. This chassis is unable to join the active virtual chassis topology whose master chassis is part of. **Mis-License-Config**: The chassis is not fully operational because its license settings do not match the master chassis' license configuration. An exact match is required to allow successful operation within the same virtual chassis topology. **Split-Topology**: The chassis is not fully operational and all of its front panel user ports (excluding the virtual-fabric link member ports) are operationally down because a topology split has occurred. This chassis became isolated from the master chassis after all of its active virtual-fabric member ports went down or the virtual chassis manager hello timeout has expired. **Running+**: Element added after last saved topology. **Not-Joined**: Element missing from last saved topology.
Chassis-Group (Group)	virtual chassis group identifier. Used to identify a group of chassis belonging to the same virtual chassis.

output definitions

Chassis-MAC (MAC-Address)	Chassis MAC address.
Up-Time	Chassis up time.
Designated-NI	Designated network interface module (NI), which is the module responsible for managing the inter-process communication infrastructure responsible for control communication between distinct switches within the virtual chassis topology. Only VFL capable network interface modules can be elected as designated NI. When no VFL capable network interface modules are present on a switch, the designated NI is zero (0).
Primary-CMM	Primary CMM slot.
Secondary-CMM	Secondary CMM slot.
Chassis-Type	The switch chassis type (OS6900 or OS6860).
License	The licenses installed on the chassis.
Hello-Interval	The hello-interval configured for the chassis.
Oper-Chassis-Priority (Pri)	Operational/current chassis priority, which defines the user preference, above all other election criteria, for a switch to become the master chassis of the virtual chassis topology. The greater this value the more likely a switch is to be elected as the master chassis.
Config-Chassis-Priority	Configured/next chassis priority, which defines the user preference above all other election criteria.
Oper-Control-VLAN	Operational/current virtual chassis control VLAN.
Config-Control-VLAN	Configured/next virtual chassis control VLAN, which will take effect after reset thereby becoming the next operational control VLAN.
Number-of-Neighbors	Total number of neighbor switches that are part of the active virtual chassis topology for a given chassis group.
VFLink Mode	The VFLink mode of the chassis: Static or Auto.
Number-of-Direct-Neighbors	Number of directly attached neighbor switches that are part of the active virtual chassis topology for a given chassis group These are switches directly connected to the local switch through a virtual-fabric link (VFL).
Neighbor	The operational chassis identifier of neighbor switch.
Is-Direct	Flag identifying whether a particular neighbor is directly attached to a given switch.
Shortest-Path	The shortest path from a given switch to a neighbor switch using the notation *chassis*/*vfl_id*.

Release History

Release 7.3.1; command introduced.
Release 7.3.4; VFLink mode introduced.

Related Commands

virtual-chassis configured-chassis-id	Assigns a globally unique chassis identifier to the switch and enables the switch to operate in virtual chassis mode.
virtual-chassis chassis-group	Assigns a globally unique chassis group identifier to a switch. Each peer switch in a virtual chassis domain must use the same group ID number.
virtual-chassis configured-chassis-priority	Sets the configured chassis priority for a switch specified by its operational chassis identifier.
virtual-chassis configured-control-vlan	Sets the configured control VLAN for a switch specified by its operational chassis identifier.
virtual-chassis configured-hello-interval	Configures the virtual chassis hello interval parameter on the switch.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasId
   virtualChassisConfigChassisID
   virtualChassisRole
   virtualChassisPreviousRole
   virtualChassisStatus
   virtualChassisConfigPriority
   virtualChassisOperPriority
   virtualChassisGroup
   virtualChassisMac
   virtualChassisUpTime
   virtualChassisDesigNI
   virtualChassisPriCmm
   virtualChassisSecCmm
   virtualChassisOperControlVlan
   virtualChassisConfigControlVlan
   virtualChassisOperHelloInterval
   virtualChassisConfigHelloInterval
   virtualChassisType
   virtualChassisLicense
   virtualChassisNumOfNeighbor
   virtualChassisNumOfDirectNeighbor
```

show virtual-chassis consistency

This command is used to provide a detailed status of the parameters taken into account to determine the consistency of a group of switches participating in the virtual chassis topology.

show virtual-chassis [chassis-id *oper_chassis***] consistency**

Syntax Definitions

oper_chassis	The operational/current chassis ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command provides a list of parameters that must be configured consistently on all switches that will participate on the virtual chassis topology to allow correct system operation.
- In order to determine the consistency of a given parameter, the switch will compare the value of such parameters on a given switch with the settings of the master chassis. Therefore consistency is always defined as a comparison with the master chassis.
- The following parameters are considered consistent if they match the settings of the master chassis: chassis type, license, chassis group, operational control VLAN, configured control VLAN, operational hello interval and configured hello interval.
- The configured chassis identifier parameter is considered consistent if it is different than the settings of the master chassis.

Examples

```
-> show virtual-chassis consistency
Legend: * - denotes mandatory consistency which will affect chassis status
        Licenses - A: Advanced; B: Data Center

       Config                                  Oper     Config
       Chas          Chas    Chas   Hello    Control  Control
 Chas* ID     Status Type*   Group* Interv   Vlan*    Vlan     License*
------+------+------+-------+------+-------+--------+--------+----------
 1     1      OK     OS6900  0      10       4094     4094     AB
 2     2      OK     OS6900  0      10       4094     4094     AB
 3     2      NOK    OS6900  0      10       4094     4000     AB
 4     2      OK     OS6900  0      10       4094     4094     AB
 5     2      OK     OS6900  0      10       4094     4094     AB
 6     2      NOK    OS6900  0      10       4094     4094     A
```

```
-> show virtual-chassis chassis-id 2 consistency
Legend: * - denotes mandatory consistency which will affect chassis status
        Licenses - A: Advanced; B: Data Center

                      Given      Master
Consistency           Chassis    Chassis   Status
--------------------+----------+----------+---------
Chassis-ID*           2          1         OK
Config-Chassis-ID     2          1         OK
Chassis-Type*         OS6900     OS6900    OK
License*              A          AB        NOK
Chassis-Group*        0          0         OK
Hello-Interval        10         10        OK
Oper-Control-Vlan*    4094       4094      OK
Config-Control-Vlan   4094       4094      OK
```

output definitions

Chassis-ID (Chas)	Operational/current virtual chassis chassis identifier. The operational chassis identifier when a switch operates in standalone mode is zero (0).
Config-Chassis-ID (Conf Chas ID)	The configured/next chassis identifier for the switch specified by operational chassis identifier.
Chassis-Type (Chas Type)	The switch chassis type (OS6900 or OS6860).
License	The licenses installed on the chassis.
Chassis-Group (Chas Group)	virtual chassis group identifier. Used to identify a group of chassis belonging to the same active virtual chassis topology.
Hello-Interval	Operational/current hello-interval.
Oper-Control-VLAN	Operational/current virtual chassis control VLAN.
Config-Control-VLAN	Configured/next virtual chassis control VLAN, which will take effect after reset thereby becoming the next operational control VLAN.
Status	Defines whether a given switch's parameter is considered consistent with the master chassis' settings. The possible values are: **OK**: The switch is operating in virtual chassis mode and the given switch's parameter value is consistent with the settings of the master chassis. **NOK**: The switch is operating in virtual chassis mode and the given switch's parameter value is inconsistent with the settings of the master chassis. **N/A**: The switch is operating in virtual chassis mode, but the virtual chassis topology has not converged and therefore a master chassis is not yet known. **Disabled**: The switch is operating in standalone mode, in which there can be no virtual chassis master and hence the concept of consistency does not apply.

Release History

Release 7.3.1; command introduced.

Related Commands

virtual-chassis configured-chassis-id	Assigns a globally unique chassis identifier to the switch and enables the switch to operate in virtual chassis mode.
virtual-chassis chassis-group	Assigns a globally unique chassis group identifier to a chassis. Each peer switch in a virtual chassis domain must use the same group ID number.
virtual-chassis configured-chassis-priority	Sets the chassis priority for a chassis specified by its operational chassis identifier.
virtual-chassis configured-control-vlan	Sets the configured control VLAN for a chassis specified by its operational chassis identifier.
virtual-chassis configured-hello-interval	Sets the configured hello interval parameter on the switch.

MIB Objects

```
virtualChassisGlobalTable
   virtualChassisOperChasId
   virtualChassisConfigChassisID
   virtualChassisType
   virtualChassisLicense
   virtualChassisGroup
   virtualChassisOperControlVlan
   virtualChassisConfigControlVlan
   virtualChassisOperHelloInterval
   virtualChassisConfigHelloInterval
```

show virtual-chassis vf-link

Displays a summary of the configured and operational parameters related to the virtual fabric links on the virtual chassis topology.

show virtual-chassis [chassis-id *oper_chassis***] vf-link** *vfl_id* **member-port [***oper_chassis/***]***slot/port*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
vfl_id	The VFL identifier.
oper_chassis/slot/port	The operational chassis identifier, slot, and port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command can be executed on any switch within the virtual chassis topology.

Examples

```
-> show virtual-chassis vf-link
VFLink mode: static
Chassis/VFLink ID  Oper       Primary Port       Config Port   Active Port Def Vlan
-------------------+----------+------------------+-------------+-------------+-----
1/0                Up         1/1/3              2             2             1
2/0                Up         2/1/3              2             2             1

-> show virtual-chassis chassis-id 1 vf-link
Chassis/VFLink ID  Oper       Primary Port       Config Port  Active Port Def Vlan
-------------------+----------+------------------+------------+----------+--------
1/0                Up         1/1/3              2             2             1

-> show virtual-chassis vf-link member-port
Chassis/VFLink ID  Chassis/Slot/Port  Oper       Is Primary
-------------------+------------------+----------+-------------
1/0                1/1/1              Up         No
1/0                1/1/3              Up         Yes
2/0                2/1/1              Up         No
2/0                2/1/3              Up         Yes

-> show virtual-chassis chassis-id 1 vf-link member-port
 Chassis/VFLink ID  Chassis/Slot/Port  Oper       Is Primary
-------------------+------------------+----------+-------------
1/0                1/1/1              Up         No
1/0                1/1/3              Up         Yes
```

output definitions

Chassis/VFLink ID	Pair operational/current virtual chassis chassis identifier and virtual-fabric link (VFL) identifier.
Oper	Virtual-fabric link (VFL) operational status. The possible values are **Up** and **Down**.
Primary Port	Primary port of the virtual-fabric link (VFL) trunk, which is the port where non-unicast packets destined a remote chassis are sent out.
Config Port	Number of ports configured to operate as virtual-fabric link (VFL) member ports, i.e. ports that potentially may join a virtual-fabric link (VFL).
Active Port	Number of virtual-fabric link (VFL) member ports that are operational, i.e. the LACP protocol is fully operational for those ports.
Def Vlan	Operational default VLAN on the virtual-fabric link (VFL).
Chassis/Slot/Port	The operational *chassis/slot/port* tupple identifying a particular virtual-fabric link (VFL) member port.
Is Primary	Indicates is this port is the primary port of the VFL.

Release History

Release 7.3.1; command introduced.
Release 7.3.4; VFLink mode introduced.

Related Commands

virtual-chassis configured-chassis-id	Assigns a globally unique chassis identifier to the switch and enables the switch to operate in virtual chassis mode.
virtual-chassis vf-link create	Configures a virtual fabric link (VFL) between two peer switches. A VFL is required to enable the Virtual Chassis operation between the two switches.
virtual-chassis vf-link member-port	Configures member ports for the virtual fabric link (VFL).
virtual-chassis vf-link default-vlan	Configures the default VLAN for the VFL.

MIB Objects

```
virtualChassisLinkTable
   virtualChassisOperChasID
   virtualChassisLinkOperDefaultVlan
   virtualChassisLinkLinkOperStatus
   virtualChassisLinkPrimaryPort
   virutalChassisLinkConfigPortNum
   virtualChassisLinkActivePortNum
   virtualChassisLinkId
   virtualChassisVflMemberPortIfindex
   virtualChassisVflMemberPortRowStatus
```

show virtual-chassis auto-vf-link-port

Displays a summary of the auto VFL ports.

show virtual-chassis [chassis-id *oper_chassis***] auto-vf-link-port [***chassis/slot/port***]**

Syntax Definitions

oper_chassis	The operational/current chassis ID number.
oper_chassis/slot/port	The operational chassis identifier, slot, and port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

This command can be executed on any switch within the virtual chassis topology.

Examples

```
-> show virtual-chassis auto-vf-link-port
Chassis/Slot/Port    VFL ID            VFL member status
-------------------+-----------------+-----------------------
1/1/1                1/0                Down
1/1/3                1/1                Up
```

output definitions

Chassis/Slot/Port	The chassis/slot/port identifier.
VFL ID	The VFL identifier.
VFL member status	The status of the VFL member port. Up or Down.

Release History

Release 7.3.4; command introduced.

Related Commands

virtual-chassis auto-vf-link-port	Configures the port to be an automatic VFL port.

MIB Objects

```
virtualChassisLinkTable
   virtualChassisOperChasID
   virtualChassisVflMemberPortRowStatus
```

show virtual-chassis chassis-reset-list

This command displays the list of all chassis that must be reset along with a specified chassis in order to prevent a virtual chassis topology split.

show virtual-chassis [chassis-id *oper_chassis***] chassis-reset-list**

Syntax Definitions

oper_chassis	The operational/current chassis ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When no operational chassis identifier is specified the command will show data related to the entire virtual chassis system.

Examples

```
->  show virtual-chassis chassis-reset-list
Chas  Chassis reset list
-----+--------------------
1     1
2     2

-> show virtual-chassis chassis-id 1 chassis-reset-list
Chas  Chassis reset list
-----+--------------------
1     1
```

output definitions

Chas	Operational/current virtual chassis chassis identifier. The operational chassis identifier when a switch operates in standalone mode is zero (0).
Chassis reset list	A list of operational chassis identifiers, which define which switches must be reset, along with the switch given by Chas in order to prevent a split of the virtual chassis topology.

Release History

Release 7.3.1; command introduced.

Related Commands

show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology

MIB Objects

```
virtualChassisChassisResetListTable
   virtualChassisOperChasId
   virtualChassisChassisResetList
```

show virtual-chassis slot-reset-list

For a given chassis and network interface module (NI), this command displays status information specifying whether bringing down or extracting such network interface module (NI) will lead to a virtual chassis topology split.

show virtual-chassis [chassis-id *oper_chassis***] slot-reset-list**

Syntax Definitions

oper_chassis	The operational/current chassis ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When no operational chassis identifier is specified the command will show data related to the entire virtual chassis system.
- On the OmniSwitch 6900, the slot number depicted in this command always refers to the main board of the switch (i.e. slot number 1). In other words, this command does not present the status related to expansion boards.

Examples

```
-> show virtual-chassis slot-reset-list
Chas  Slot    Reset status
-----+-------+--------------
1     1       Split
2     1       Split

-> show virtual-chassis chassis-id 1 slot-reset-list
Chas  Slot    Reset status
-----+-------+--------------
1     1       Split
```

output definitions

Chas	Operational/current virtual chassis chassis identifier. The operational chassis identifier when a switch operates in standalone mode is zero (0).

output definitions

Slot	Slot number identifying a particular network interface module (NI). For OS6900 switches, the slot number is always be equal to 1.
Reset Status	For the network interface module (NI) identified by the pair (Chas, Slot), this command displays status information specifying whether bringing down or extracting such network interface module (NI) will lead to a virtual chassis topology split according to the following definitions. **Supported**: The network interface module can be reset without splitting the virtual chassis topology. **Split**: Resetting this network interface module will cause a virtual chassis topology split.

Release History

Release 7.3.1; command introduced.

Related Commands

show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology

MIB Objects

```
virtualChassisSlotResetStatusTable
   virtualChassisOperChasID
   virtualChassisSlotResetStatus
```

show virtual-chassis neighbors

This command displays a list of which neighbors are connected via which VFL for a virtual chassis.

show virtual-chassis [chassis-id *oper_chassis***] neighbors**

Syntax Definitions

oper_chassis	The operational/current chassis ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When no operational chassis identifier is specified the command will show data related to the entire virtual chassis system.

Examples

```
-> show virtual-chassis neighbors

Chas VFL VFL VFL VFL VFL
 ID   0   1   2   3   4
----+---+---+---+---+---
  1   2   3   4   5   6
  2   1   3   4   5   6
  3   1   2   4   5   6
  4   1   2   3   5   6
  5   1   2   3   4   6
  6   1   2   3   4   5

-> show virtual-chassis chassis-id 2 neighbors

Chas VFL VFL VFL VFL VFL
 ID   0   1   2   3   4
----+---+---+---+---+---
  2   1   3   4   5   6
```

output definitions

Chas ID	Operational/current virtual chassis chassis identifier. The operational chassis identifier when a switch operates in standalone mode is zero (0).
VFL	The VLF identifier connecting to the remote chassis listed in the table.

Release History

Release 7.3.3; command introduced.

Related Commands

show virtual-chassis topology	Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology

MIB Objects

```
virtualChassisVflTable
   virtualChassisOperChasID
   virtualChassisVflId
   virtualChassisVflDirectNeighborChasId
```

show configuration vcm-snapshot chassis-id

Displays a snapshot of the switch specific virtual chassis configuration for a switch running in virtual chassis mode.

show configuration vcm-snapshot chassis-id *oper_chassis*

Syntax Definitions

oper_chassis	The operational/current chassis ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When a switch operates in standalone mode, this command is not supported. In this case, we must use the **show configuration snapshot virtual chassis** to obtain a snapshot of the switch specific virtual chassis configuration.

Examples

```
-> show configuration vcm-snapshot chassis-id 1
! Virtual Chassis Manager:
virtual-chassis chassis-id 1 configured-chassis-id 1
virtual-chassis chassis-id 1 vf-link 0 create
virtual-chassis chassis-id 1 vf-link 0 member-port 1/8/1
virtual-chassis chassis-id 1 configured-control-vlan 4091
virtual-chassis chassis-id 1 chassis-group 1

! IP:
ip interface local chassis-id 1 emp address 10.255.76.21 mask 255.255.255.0
```

Release History

Release 7.3.1; command introduced.

Related Commands

show configuration snapshot	Displays the configured and operational parameters related to the virtual chassis feature on the switch.

MIB Objects

N/A

virtual-chassis split-protection admin-state

Enable or disables the VC split protection feature.

virtual-chassis split-protection admin-state {enable | disable}

Syntax Definitions

enable	Enables VC split protection.
disable	Disables VC split protection.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- VCSP cannot be enabled before assigning a link aggregate.
- VCSP and the helper functionality can be enabled on the same link aggregate.
- The virtual chassis and its helper cannot have the same Group ID.

Examples

```
-> virtual-chassis split-protection admin-state enable
-> virtual-chassis split-protection admin-state disable
```

Release History

Release 7.3.4.R02; command was introduced.

Related Commands

show virtual-chassis split-protection status	Displays all the information related to VCSP when enabled.
virtual-chassis split-protection linkagg	Assigns a link aggregate for use with VCSP.

MIB Objects

```
alaVCSPConfigInfo
   alaVCSPAdminState
```

virtual-chassis split-protection linkagg

Assigns a link aggregate for use with VCSP.

virtual-chassis split-protection linkagg *agg_id*

no virtual-chassis split-protection linkagg

Syntax Definitions

agg_id	The link aggregate ID number to associate with the helper for VCSP support. The valid range is 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the link aggregate assignment.
- This command must be used to configure VC split protection linkagg before enabling VC split protection.

Examples

```
-> virtual-chassis split-protection linkagg 1
```

Release History

Release 7.3.4.R02; command was introduced.

Related Commands

show virtual-chassis split-protection status	Displays all the information related to VCSP when enabled.

MIB Objects

```
alaVCSPConfigInfo
   alaVCSPLinkaggID
```

virtual-chassis split-protection guard-timer

Configures the timer value for how long the master will wait to receive VCSP PDUs before beginning transmission of VCSP PDUs.

virtual-chassis split-protection guard-timer *time*

Syntax Definitions

time	Time interval to wait on boot up before choosing any state. The valid range is 30–100 seconds.

Defaults

parameter	default
time	30 seconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Changes to the Guard timer only take affect after reboot or by disabling and re-enabling VC split protection.

Examples

```
-> virtual-chassis split-protection guard-timer 60
```

Release History

Release 7.3.4.R02; command was introduced.

Related Commands

show virtual-chassis split-protection status	Displays all the information related to VCSP when enabled.

MIB Objects

```
alaVCSPConfigInfo
   alaVCSPGuardTimer
```

virtual-chassis split-protection helper admin-state

Enables or disables the helper functionality on the helper device.

virtual-chassis split-protection helper admin-state {enable | disable}

Syntax Definitions

enable	Enables VC split protection helper functionality.
disable	Disables VC split protection helper functionality.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command on the helper device to enable the helper functionality.
- The helper functionality can be enabled on a device that is running VCSP.
- The virtual chassis and its helper cannot have the same Group ID.

Examples

```
-> virtual-chassis split-protection helper admin-state enable
-> virtual-chassis split-protection helper admin-state disable
```

Release History

Release 7.3.4.R02; command was introduced.

Related Commands

virtual-chassis split-protection helper linkagg	Configures the link aggregate on which to apply the VCSP protocol for the helper device.

MIB Objects

```
alaVCSPHelperGlobalConfig
   alaVCSPHelperAdminState
```

virtual-chassis split-protection helper linkagg

Configures the link aggregate ID on which to apply the VCSP protocol on the helper device.

virtual-chassis split-protection helper linkagg *agg_id*

no virtual-chassis split-protection helper linkagg

Syntax Definitions

agg_id	The link aggregate ID number to associate with the helper for VCSP support. The valid range is 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the link aggregate assignment.
- Use this command on the helper device to enable the VCSP protocol on the helper link aggregate.

Examples

```
-> virtual-chassis split-protection helper linkagg 1
-> no virtual-chassis split-protection helper linkagg
```

Release History

Release 7.3.4.R02; command was introduced.

Related Commands

show virtual-chassis split-protection status	Displays the VCSP Helper status of the Link Aggregation ID assigned.
virtual-chassis split-protection helper admin-state	Enables or disables to helper functionality.

MIB Objects

```
alaVCSPHelperLinkaggTable
   alaVCSPHelperLinkaggId
   alaVCSPHelperLinkaggRowStatus
```

show virtual-chassis split-protection status

Displays all the information related to VCSP when enabled.

show virtual-chassis split-protection status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show virtual-chassis split-protection status
VCSP admin status:       enabled
VCSP operational status: Active
VCSP linkagg:            31
VCSP Guard Timer:        30
VCSP Uptime:             00d:00h:00m:00s,
VCSP Protection Uptime:  00d:00h:00m:00s
```

Release History

Release 7.3.4.R02; command was introduced.

Related Commands

virtual-chassis split-protection admin-state	Enable or disables the VC split protection feature.

MIB Objects

```
alaVCSPConfigInfo
   alaVCSPAdminState
   alaVCSPOperState
   alaVCSPLinkaggId
   alaVCSPGuardTimer
   alaVCSPUptime
   alaVCSPProtectionStateUptime
```

show virtual-chassis split-protection vc-units

Displays the VCSP state of all VC units.

show virtual-chassis split-protection vc-units

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show virtual-chassis split-protection vc-units

CHASSIS     STATE
----------+-----------
 1          ACTIVE
 2          ACTIVE
```

Release History

Release 7.3.4.R02; command was introduced.

Related Commands

virtual-chassis split-protection admin-state	Enable or disables the VC split protection feature.

MIB Objects

```
alaVCSPStateTable
   alaVCSPTableSlotNiNumber
   alaVCSPTableOperState
```

show virtual-chassis split-protection helper status

Displays the VCSP Helper status of the assigned link aggregation ID.

show virtual-chassis split-protection helper status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show virtual-chassis split-protection helper status
VC Split-Protection Helper Status : Enabled
 Link Aggregation Id            VC Split-Protection Status
------------------------+-------------------------------------------------------
           3                        Enabled
```

Release History

Release 7.3.4.R02; command was introduced.

Related Commands

virtual-chassis split-protection helper admin-state	Enables or disables the helper functionality.

MIB Objects

```
alaVCSPHelperGlobalConfig
   alaVCSPHelperLinkaggId
   alaVCSPHelperState
```

14 Ethernet Ring Protection Commands

Ethernet Ring Protection (ERP) is a protection switching mechanism for Ethernet ring topologies, such as multi-ring and ladder networks. The implementation of ERP on the OmniSwitch is based on ERP Version 2 (ITU-T G.8032/Y.1344 to 2010) using the Ring Automatic Protection Switching (R-APS) protocol to coordinate and prevent network loops within a bridged Ethernet ring.

ERPv2 supports multi-rings and ladder to ladder networks. ERPv2 functionalities allow configuration of Sub-Rings within a Master Ethernet Ring, interconnected nodes and shared links between the rings.

MIB information for Ethernet Ring Protection commands is as follows:

Filename: ALCATEL-IND1-ERP-MIB.mib
Module: alcatelIND1ERPMIB

A summary of available commands is listed here:

erp-ring

Creates an Ethernet Ring Protection (ERP) using the specified ports and service VLAN ID. The service VLAN transmits ERP control traffic, such as Ring Automatic Protection Switching (R-APS) messages, through the ring. The specified level number identifies an APS Management Entity Group (MEG) to which the service VLAN belongs.

erp-ring *ring_id* **port1 {***chassis/slot/port* **| linkagg** *agg_id***} port2 {***chassis/slot/port* **| linkagg** *agg_id***} service-vlan** *vlan_id* **level** *level_num* **[guard-timer** *guard_timer***] [wait-to-restore-timer** *wtr_timer***] [enable | disable]**

no erp-ring *ring_id*

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
agg_id	The link aggregate ID number.
vlan_id	The service VLAN ID number.The valid range is 1 to 4094.
level_num	The MEG level number for the service VLAN. The valid range is 0 to 7.
guard-timer	The guard timer value, in centi seconds, for the ring node.
wtr-timer	The wait-to-restore timer value, in minutes, for the Ring Protection Link (RPL) node.
enable	Administratively enables the ERP ring**.**
disable	Administratively disables the ERP ring.

Defaults

parameter	default
guard_timer	50
wtr_timer	5
**enable	disable**	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a ring from the switch configuration. Administratively disable the ring ports before deleting the ring to avoid creating any network loops. Once the ring is deleted, ensure that the same ports are administratively enabled under Spanning Tree control.
- The specified ring identification number must be unique within a switch.

- ERP is not supported on mobile ports, mirroring ports, link aggregate member ports, high availability ports, Multicast VLAN receiver ports (ERP is supported on Multicast VLAN sender ports only), VLAN Stacking user network interface (UNI) ports, or RRSTP ring ports.
- If a port is tagged with the service VLAN ID or the service VLAN is the default VLAN for the port, then the port is not eligible to become an ERP ring port.
- Specify an existing VLAN ID for the service VLAN ID. Use the same VLAN ID and level number for the service VLAN on each switch that participates in the ERP ring.
- If the ERP switch participates in an Ethernet OAM Maintenance Domain (MD), configure the ERP service VLAN to use the same level number that is used for the Ethernet OAM MD.
- Specify a static VLAN ID for the ERP service VLAN; dynamic VLANs are not configurable as service VLANs.
- The service VLAN can belong to only one ERP ring at a time. A maximum of 64 rings are allowed per switch.
- The specified service VLAN ID must not participate in a Spanning Tree instance that is associated with non-ERP VLANs. Ideally, change the Spanning Tree configuration for the VLAN ID prior to using this command.
- An ERP ring port can belong to only one ERP ring at a time.
- Create an ERP type NNI-SVLAN binding before establishing an ERP ring on that SVLAN-NNI binding.

Examples

```
-> erp-ring 1 port1 1/1 port2 2/4 service-vlan 10 level 2 enable
-> erp-ring 2 port1 linkagg 1 port2 2/10 service-vlan 20 level 2
-> erp-ring 3 port1 linkagg 2 port2 linkagg 4 service-vlan 30 level 7
-> no erp-ring 2
```

Release History

Release 7.1.1; command introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.
ethernet-service svlan nni	Creates an NNI-SVLAN binding.

MIB Objects

```
alaErpRingTable
   alaErpRingServiceVid
   alaErpRingMEGLevel
   alaErpRingStatus
   alaErpRingPort1
   alaErpRingPort2
   alaErpRingWaitToRestore
   alaErpRingGuardTimer
   alaErpRingRowStatus
```

erp-ring rpl-node

Configures a switch as a Ring Protection Link (RPL) node. This command also identifies the ERP port as an RPL connection port. The RPL remains blocked to prevent loops within the ERP ring.

erp-ring *ring_id* **rpl-node {port** *chassis/slot/port* **| linkagg** *agg_id***}**

no erp-ring *ring_id* **rpl-node**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
agg_id	The link aggregate ID number.

Defaults

NA

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the RPL designation for the specified ring.
- The RPL node can be configured only when the ring is disabled. RPL configuration applied to the Ethernet ring while it is enabled is rejected.
- The specified ERP ring ID must exist in the switch configuration.
- This command applies only to ERP ring ports; ports not configured as ERP ring ports are not eligible to become RPL ports.
- Only one of the two ring ports configured for the switch can be designated as an RPL node port.

Examples

```
-> erp-ring 1 rpl-node port 2/1
-> erp-ring 2 rpl-node linkagg 2
-> no erp-ring 2 rpl-node
```

Release History

Release 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
erp-ring wait-to-restore	Configures the wait-to-restore timer value for the Ring Protection Link (RPL) node.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingPortEntry
   alaErpRingPortIfIndex
   alaErpRingPortType
```

erp-ring wait-to-restore

Configures the wait-to-restore timer value for the Ring Protection Link (RPL) switch. This timer determines the number of minutes the RPL switch waits before returning the RPL ports to a blocked state after the ERP ring has recovered from a link failure.

erp-ring *ring_id* **wait-to-restore** *wtr_timer*

no erp-ring *ring_id* **wait-to-restore**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
wtr_timer	The number of minutes to wait before restoring the RPL to a blocked state. The valid range is 1 to 12.

Defaults

By default, the wait-to-restore timer value is set to 5 minutes.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to set the timer back to the default setting of 5 minutes.
- The specified ERP ring ID must exist in the switch configuration.
- This command applies only on a switch that serves as the RPL node for the ERP ring.

Examples

```
-> erp-ring 1 wait-to-restore 6
-> no erp-ring 1 wait-to-restore
```

Release History

Release 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
erp-ring rpl-node	Configures a Ring Protection Link (RPL) port connection.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId
   alaErpRingWaitToRestoreTimer
```

erp-ring enable

Enables or disables an ERP ring identified by the specified ring ID. This command applies to enabling or disabling existing ERP rings.

erp-ring *ring_id* **{enable** | **disable}**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
enable	Enables the specified ring ID.
disable	Disables the specified ring ID.

Defaults

By default, ERP rings are disabled when they are created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- The specified ring ID must exist in the switch configuration.
- Enabling a ring is also allowed at the time the ring is created.

Examples

```
-> erp-ring 1 enable
-> erp-ring 1 disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId
   alaErpRingStatus
```

erp-ring guard-timer

Configures the guard timer value for the specified ERP ring node. The guard timer is used to prevent ring nodes from receiving outdated Ring Automatic Protection Switching (R-APS) messages. During the amount of time determined by this timer, all received R-APS messages are ignored by the ring protection control process.

erp-ring *ring_id* **guard-timer** *guard_timer*

no erp-ring *ring_id* **guard-timer**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
guard_timer	The guard timer value. The valid range is 1–200 centi-secs.

Defaults

parameter	default
guard_timer	50

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to set the timer back to the default value of 50 centi-secs.
- The specified ring ID must exist in the switch configuration.

Examples

```
-> erp-ring 1 guard-timer 10
-> no erp-ring 1 guard-timer
```

Release History

Release 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId
   alaErpRingGuardTimer
```

erp-ring sub-ring

Creates an Ethernet Ring Protection (ERP) sub-ring.

erp-ring *ring_id* **sub-ring-port {***chassis/slot/port* **| linkagg** *agg_id***} service-vlan** *vlan_id* **level** *level_num* **[guard-timer** *guard_timer***] [wait-to-restore-timer** *wtr_timer***] [enable | disable]**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
agg_id	The link aggregate ID number.
vlan_id	The service VLAN ID number.The valid range is 1 to 4094.
level_num	The MEG level number for the service VLAN. The valid range is 0 to 7.
guard_timer	The guard timer value, in centi-secs, for the ring node.
wtr-timer	The wait-to-restore timer value, in minutes, for the Ring Protection Link (RPL) node.
enable	Administratively enables the ERP sub-ring**.**
disable	Administratively disables the ERP sub-ring.

Defaults

parameter	default
guard_timer	50
wtr_timer	5
**enable	disable**	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a sub-ring from the switch configuration. Administratively disable ring ports before deleting the ring to avoid creating any network loops. Once the ring is deleted, ensure that the same ports are administratively enabled under Spanning Tree control.
- The specified ring identification number must be unique within a switch.
- ERP is not supported on mobile ports, mirroring ports, link aggregate member ports, high availability ports, Multicast VLAN receiver ports (ERP is supported on Multicast VLAN sender ports only), VLAN Stacking user network interface (UNI) ports, or RRSTP ring ports.

- If a port is tagged with the service VLAN ID or the service VLAN is the default VLAN for the port, the port is not eligible to become an ERP ring port.
- Specify an existing VLAN ID for the service VLAN ID. Use the same VLAN ID and level number for the service VLAN on each switch that participates in the ERP ring.
- If the ERP switch participates in an Ethernet OAM Maintenance Domain (MD), configure the ERP service VLAN to use the same level number that is used for the Ethernet OAM MD.
- Specify a static VLAN ID for the ERP service VLAN; dynamic VLANs are not configurable as service VLANs.
- The service VLAN can belong to only one ERP ring at a time. A maximum of four rings are allowed per switch.
- The specified service VLAN ID must not participate in a Spanning Tree instance that is associated with non-ERP VLANs. Ideally, change the Spanning Tree configuration for the VLAN ID prior to using this command.
- An ERP ring port can belong to only one ERP ring at a time.
- An ERP type NNI-SVLAN binding must be created before establishing an ERP ring on that SVLAN-NNI binding.

Examples

```
-> erp-ring 1 sub-ring-port 1/1 service-vlan 10 level 2 enable
-> erp-ring 2 sub-ring-port linkagg 1 port2 2/10 service-vlan 20 level 2
-> no erp-ring 2
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.
ethernet-service svlan nni	Creates a NNI-SVLAN binding.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingServiceVid
   alaErpRingMEGLevel
   alaErpRingStatus
   alaErpRingPort1
   alaErpRingPort2
   alaErpRingWaitToRestore
   alaErpRingGuardTimer
   alaErpRingRowStatus
```

erp-ring virtual-channel

Enables or disables an Ethernet Ring Protection (ERP) Ring Virtual Channel.

erp-ring *ring_id* **virtual-channel [enable | disable]**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
enable	Administratively enables the ERP virtual channel**.** If enabled, Ring Automatic Protection Switching (R-APS) protocol messages are encapsulated and transmitted over a virtual channel configured on the major ring.
disable	Administratively disables the ERP virtual channel. If disabled, R-APS messages are terminated at the interconnection nodes between the rings but not blocked at the Ring Protection Link (RPL) of the sub-ring.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- The specified ring identification number must be unique within a switch.
- The ring identified by Ring ID must be created before configuring the virtual channel state for ring node.

Examples

```
-> erp-ring 2 virtual-channel disable
-> erp-ring 1 virtual-channel enable
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingVirtualChannel
```

erp-ring revertive

Enables or Disables revertive mode on the specified node.

erp-ring *ring_id* **revertive [enable | disable]**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
enable	Administratively enables Revertive Mode**.** Now, if the RPL is unblocked due to a failure within the ring, the RPL automatically reverts to the “Blocked” state when the failed link recovers.
disable	Administratively Disables Revertive Mode.Now, if the RPL is unblocked due to a failure within the ring, the RPL does not automatically revert to “Blocked” state when the failed link recovers.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- The specified ring identification number must be unique within a switch.
- The ring identified by the Ring ID must be created using the **erp-ring** command, before configuring the revertive mode for ring node.

Examples

```
-> erp-ring 1 revertive enable
-> erp-ring 2 revertive disable
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
erp-ring clear	Clears any pending state (for example, non-revertive restoring).
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingRevertive
```

erp-ring clear

Clears any pending state (for example, non-revertive restoring).

erp-ring *ring_id* **clear**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
clear	Clears any pending state on the ring.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

The specified ring identification number must be unique within a switch.

Examples

```
-> erp-ring 1 clear
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingClearAction
```

erp-ring ethoam-event

Configures a ring port to accept a “loss of connectivity” event from Ethernet OAM for a remote endpoint.

erp-ring *ring_id* **ethoam-event {***chassis/slot/port* **| linkagg** *agg_id***} remote-endpoint** *mep_id*

no erp-ring *ring_id* **ethoam-event {***chassis/slot/port* **| linkagg** *agg_id***}**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1 to 2147483647.
chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
agg_id	The link aggregate ID number.
mep_id	The remote endpoint ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

The specified ring identification number must be unique within a switch.

Examples

```
-> erp-ring 1 ethoam-event 1/1 remote-endpoint 10
-> erp-ring 1 ethoam-event linkagg 1 remote-endpoint 10
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingPortIfIndex
   alaErpRingPortEthOAMEvent
   alaErpRingPortRmepId
```

clear erp statistics

Clears ERP statistics for all rings, a specific ring, or a specific ring port.

clear erp statistics [ring *ring_id* **[port** *chassis/slot/port* **| linkagg** *agg_id***]]**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
agg_id	The link aggregate ID number.

Defaults

By default, statistics are cleared for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Enter a ring ID to clear the statistics for a specific ring.
- Enter a ring ID and a ring port number or link aggregate ID to clear the statistics for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.
- The specified port must belong to the ring identified by the ring ID.

Examples

```
-> clear erp statistics
-> clear erp statistics ring 5
-> clear erp statistics ring 5 port 1/2
-> clear erp statistics ring 5 linkagg 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpClearStats
alaErpRingTable
   alaErpRingId
   alaErpRingClearStats
alaErpRingPortTable
   alaErpRingPortIfIndex
   alaErpRingPortClearStats
```

show erp

Displays the ERP configuration information for all rings, a specific ring, or for a specific ring port.

show erp [ring *ring_id* **| [port** *chassis/slot/port* **| linkagg** *agg_id***]]**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
agg_id	The link aggregate ID number.

Defaults

By default, configuration information is displayed for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Enter a ring ID to display the configuration for a specific ring.
- Enter a ring port number or a link aggregate ID to display the configuration for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.

Examples

```
-> show erp
Legends: *    to Inactive Configuration
         WTR  to Wait To Restore
         MEG  to Maintenance Entity Group

  Ring      Ring  Ring    Ring     Serv  WTR  Guard  MEG        Ring      Ring
   ID       Port1 Port2   Status   VLAN Timer Timer Level       State     Node
                                      (min) (csec)
----------+------+------+---------+----+-----+-----+-----+-----------+--------
         1   1/15    1/1   enabled 4094    3    50     2         idle      rpl
         2    6/7    4/1   enabled 4093    1    50     1         idle      rpl
         3    4/7    6/1   enabled 4092    1    50     3         idle      rpl
         4    4/8   6/23   enabled 4091    5    50     4         idle  non-rpl

Total number of rings configured = 4


-> show erp ring 1
Legend: *   to Inactive Configuration

Ring Id                : 1,
```

```
Ring Port1              : 1/15,
Ring Port2              : 1/1,
Ring Status             : enabled,
Service VLAN            : 4094,
WTR Timer (min)         : 3,
Guard Timer (centi-sec) : 50,
MEG Level               : 2,
Ring State              : idle,
Ring Node Type          : rpl,
RPL Port                : 1/1,
Last State Change       : SUN DEC 25 06:50:17 2016 (sysUpTime 00h:01m:31s)
```

output definitions

Ring ID	The ERP ring ID number.
Ring Ports	The slot and port number of the ring ports.
Ring Status	The ring status **(enabled** or **disabled)**.
Service VLAN	The Service VLAN ID.
WTR Timer	The wait-to-restore timer value in minutes for RPL node.
Guard Timer	The guard timer value in centi-secs for the ring node.
MEG Level	The Service VLAN Management Entity Group (MEG) level.
Ring State	Indicates the state of the ring.
Ring Node Type	Indicates the type of the ring node.
Last State Change	Indicates the time when the last state change occurred.

```
-> show erp port 1/15
Legend: *  to Inactive Configuration

Ring-Id : 1
  Ring Port Status     : forwarding,
  Ring Port Type       : non-rpl,
  Ethoam Event         : disabled


-> show erp port 1/1
Legend: *  to Inactive Configuration

Ring Id : 1
  Ring Port Status     : blocking,
  Rint Port Type       : RPL,
  Ethoam Event         : enabled,
  Rmepid               : 10
```

output definitions

Ring ID	The ERP ring ID number.
Ring Port Status	The status of the ring port (**blocking** or **forwarding**).
Ring Port Type	The type of ring port (**RPL** or **non-RPL**).
Ethoam Event	Indicates whether or not the ring port will accept Ethernet OAM loss of connectivity events (**enabled** or **disabled)**.
Rmepid	The remote Ethernet OAM MEP ID number from which this port accepts loss of connectivity events. This field displays only when the ring port is configured to receive such events.

Release History

Release 7.1.1; command introduced.

Related Commands

show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingId
   alaErpRingStatus
   alaErpRingServiceVid
   alaErpRingMEGLevel
   alaErpRingPort1
   alaErpRingPort2
   alaErpRingPortIfIndex
   alaErpRingState
   alaErpRingPortStatus
   alaErpRingPortType
   alaErpRingPortEthOAMEvent
   alaErpRingPortRmepId
   alaErpRingWaitToRestoreTimer
   alaErpRingGuardTimer
   alaErpRingLastStateChange
   alaErpRingTimeToRevert
```

show erp statistics

Displays the ERP statistics for all rings, a specific ring, or a specific ring port.

show erp statistics [ring *ring_id* **[port** *chassis/slot/port* **| linkagg** *agg_id***]]**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1 to 2147483647.
chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
agg_id	The link aggregate ID number.

Defaults

By default, statistics are displayed for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Enter a ring ID to display the statistics for a specific ring.
- Enter a ring ID and a ring port number or link aggregate ID to display the statistics for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.
- The specified port must belong to the ring identified by the ring ID.

Examples

```
-> show erp statistics
Legends: R-APS  to Ring Automatic Protection Switching
         RPL    to Ring Protection Link

Ring-Id : 1
  Ring Port : 1/15
    Signal Fail PDUs
      Sent : 3,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 37,
      Recv : 37,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4322,
      Recv : 0,
      Drop : 0
```

```
      Invalid R-APS PDUs
        Recv : 0

    Ring Port : 1/1
      Signal Fail PDUs
        Sent : 6,
        Recv : 0,
        Drop : 0
      No Request PDUs
        Sent : 37,
        Recv : 38,
        Drop : 0
      No Request RPL Block PDUs
        Sent : 4322,
        Recv : 0,
        Drop : 0
      Invalid R-APS PDUs
        Recv : 0

Ring-Id : 2
  Ring Port : 6/7
    Signal Fail PDUs
      Sent : 6,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 16,
      Recv : 14,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4347,
      Recv : 0,
      Drop : 4341
    Invalid R-APS PDUs
      Recv : 0

-> show erp statistics ring 3
Legends: R-APS  to Ring Automatic Protection Switching
         RPL    to Ring Protection Link

Ring-Id : 3
  Ring Port : 4/7
    Signal Fail PDUs
      Sent : 6,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 16,
      Recv : 14,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4351,
      Recv : 0,
      Drop : 0
    Invalid R-APS PDUs
      Recv : 0

    Ring Port : 6/1
```

```
    Signal Fail PDUs
      Sent : 6,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 13,
      Recv : 13,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4358,
      Recv : 0,
      Drop : 0
    Invalid R-APS PDUs
      Recv : 0


-> show erp statistics ring 1 port 1/15
Legends: R-APS  to Ring Automatic Protection Switching
         RPL    to Ring Protection Link

Ring-Id : 1
  Ring Port : 1/15
    Signal Fail PDUs
      Sent : 3,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 37,
      Recv : 37,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4338,
      Recv : 0,
      Drop : 0
    Invalid R-APS PDUs
      Recv: 0
```

output definitions

Ring ID	The ERP ring ID number.
Ring Port	The slot and port number of the ring port.
R-APS	The type of Ring Automatic Switching Protocol (R-APS) event message (**NR** = no request, **RB** = RPL is blocked, **SF** = signal failure). APS is the protocol ERP uses to monitor and control ring links.
Send	Total number of R-APS messages sent.
Recv	Total number of R-APS messages received.
Drop	Total number of R-APS messages dropped.

Release History

Release 7.1.1; command introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.
clear erp statistics	Clears ERP ring statistics.

MIB Objects

```
alaERPClearStats
alaERPRingClearStats
alaErpRingPortClearStats
alaErpRingId
   alaErpRingPortIfIndex
   alaErpStatsSignalFailPduTx
   alaErpStatsSignalFailPduRx
   alaErpStatsSignalFailPduDrop
   alaErpStatsNoRequestPduTx
   alaErpStatsNoRequestPduRx
   alaErpStatsNoRequestPduDrop
   alaErpStatsRPLBlockPDUTx
   alaErpStatsRPLBlockPDURx
   alaErpStatsRPLBlockPDUDrop
   alaErpStatsPDUErr
```

15 MVRP Commands

MVRP (Multiple VLAN Registration Protocol) provides a mechanism for maintaining the contents of Dynamic VLAN Registration Entries for each VLAN, and for propagating the information they contain to other Bridges. MVRP uses MRP (Multiple Registration Protocol) as the underlying mechanism, for the maintenance and propagation of the VLAN information.

MVRP acts as an MRP application, sending and receiving MVRP information encapsulated in an Ethernet frame on a specific MAC address. MVRP allows both end stations and Bridges in a Bridged Local Area Network to issue and revoke declarations relating to membership of VLANs.

Filename: ALCATEL-IND1-MVRP-MIB.mib
Module: alcatelIND1MVRPMIB

A summary of the available commands is listed here:

mvrp

Enables or disables MVRP globally on the switch.

mvrp {enable | disable}

Syntax Definitions

enable	Enables MVRP globally on the switch.
disable	Disables MVRP globally on the switch.

Defaults

By default, MVRP is disabled on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Disabling MVRP globally deletes all the MVRP learned VLANs.
- MVRP is supported only when the switch is operating in the flat Spanning Tree mode and it is not supported in the per-VLAN mode.

Examples

```
-> mvrp enable
-> mvrp disable
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp configuration	Displays the global configuration for MVRP.

MIB Objects

```
alaMvrpGlobalStatus
```

mvrp port

Enables or disables MVRP on specific ports on the switch.

mvrp port *chassis/slot/port***[–***port2***] {enable | disable}**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8)
enable	Enables MVRP on a port.
disable	Disables MVRP on a port.

Defaults

By default, MVRP is disabled on all the ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP must be enabled globally on the switch.
- When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation.
- MVRP can be enabled only on fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports. Other ports (mirroring ports, aggregable ports, VLAN Stacking User ports) do not support MVRP.

Examples

```
-> mvrp port 1/2 enable
-> mvrp port 1/2 disable
-> mvrp port 1/1-10 enable
-> mvrp port 1/1-10 disable
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp statistics	Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortStatus
```

mvrp linkagg

Enables or disables MVRP on specific aggregates on the switch.

mvrp linkagg *agg_id***[-***agg_id2***] {enable | disable}**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables MVRP for the specified link aggregate ID.
disable	Disables MVRP for the specified link aggregate ID.

Defaults

By default, MVRP is disabled on all the ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP must be enabled globally on the switch.
- When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation.
- MVRP can be enabled only on fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports. Other ports (mirroring ports, aggregable ports, mobile ports, VPLS Access ports, VLAN Stacking User ports) do not support MVRP.
- To use the *agg_id* parameter, the link aggregate group must be created.

Examples

```
-> mvrp linkagg 10 enable
-> mvrp linkagg 10 disable
-> mvrp linkagg 2-5 enable
-> mvrp linkagg 1-5 disable
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp statistics	Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortStatus
```

mvrp maximum-vlan

Configures the maximum number of dynamic VLANs that can be created by MVRP.

mvrp maximum-vlan *vlan_limit*

Syntax Definitions

vlan_limit	The maximum number of VLANs to be created by MVRP. The valid range is 32–4094.

Defaults

The default value is 256.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command can be used even when MVRP is not enabled on the switch. However, MVRP must be enabled on the switch for creating dynamic VLANs.
- If the VLAN limit to be set is less than the current number of dynamically learned VLANs, then the new configuration takes effect only after the MVRP is disabled and re-enabled on the switch. The VLANs learned earlier are retained if this operation is not performed.

Examples

```
-> mvrp maximum-vlan 100
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp configuration	Displays the global configuration for MVRP.
show mvrp vlan-restrictions	Displays the list of VLANS learned through MVRP and their details.

MIB Objects

```
alaMvrpMaxVlanLimit
```

mvrp registration

Configures the MVRP registration mode for specific ports or aggregates.

mvrp {port *chassis/slot/port***[–** *port2***] | linkagg** *agg_id***[-***agg_id2***]} registration {normal | fixed | forbidden}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
normal	Specifies that both registration and de-registration of VLANs are allowed. VLANs can be mapped either dynamically (through MVRP) or statically (through management application) on such a port.
fixed	Specifies that only static mapping of VLANs is allowed on the port but de-registration of previously created dynamic or static VLANs is not allowed.
forbidden	Specifies that dynamic VLAN registration or de-registration is not allowed on the port. Any dynamic VLANs created earlier is de-registered.

Defaults

parameter	default
normal | fixed | forbidden	**normal**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 registration forbidden
-> mvrp port 1/5 registration normal
-> mvrp linkagg 10 registration fixed
-> mvrp linkagg 20 registration forbidden
-> mvrp port 2/5-10 registration normal
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigRegistrarMode
```

mvrp applicant

Configures the applicant mode of specific ports on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.

mvrp {port *chassis/slot/port***[–***port2***] | linkagg** *agg_id***[-***agg_id2***]} applicant {participant | non-participant | active}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
participant	Specifies that MVRP PDU exchanges are only allowed when the port is in the STP forwarding state.
non-participant	Specifies that MVRP PDU's are not sent in this mode and PDU's received are processed and learning happens as expected.
active	Specifies that MVRP PDU exchanges are allowed when the port is in the STP forwarding state or STP blocking state. This is applicable for both advertisement and registration.

Defaults

parameter	default
participant | non-participant | active	**active**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 applicant active
-> mvrp port 1/3 applicant participant
-> mvrp port 1/4 applicant non-participant
-> mvrp linkagg 10 applicant active
-> mvrp linkagg 15 applicant participant
-> mvrp linkagg 20 applicant non-participant
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigtable
   alaMvrpPortConfigApplicantMode
```

mvrp timer join

Specifies the join time interval between transmit opportunities for the dynamically registering VLANs on the switch.

mvrp {port *chassis/slot/port***[–***port2***] | linkagg** *agg_id***[-***agg_id2***]} timer join** *timer_value*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
timer_value	Specifies the value of the join timer in milliseconds. The valid range is 250 milliseconds to 1073741773 milliseconds.

Defaults

parameter	default
timer-value	600 milliseconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 timer join 600
-> mvrp port 1/2-12 timer join 600
-> mvrp linkagg 3 timer join 600
-> mvrp linkagg 3-6 timer join 600
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp timer	Displays the timer values configured for all the ports or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
```

mvrp timer leave

Specifies the period of time that the switch has to wait in the Leave state before changing to the unregistered state.

mvrp {port *chassis/slot/port***[–***port2***] | linkagg** *agg_id***[-***agg_id2***]} timer leave** *timer_value*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
timer-value	Specifies the value of the Leave Timer in milliseconds. The valid range is 750 milliseconds to 2147483647 milliseconds.

Defaults

parameter	default
timer_value	1800 milliseconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- Leave timer value must be greater than or equal to twice the Join timer value, plus six times the timer resolution (16.66 milliseconds). Leave timer must be at least be greater than twice the join timer plus100 milliseconds.
- To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 timer leave 1800
-> mvrp port 1/2-12 timer leave 1800
-> mvrp linkagg 3 timer leave 1800
-> mvrp linkagg 3-6 timer leave 1800
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp timer	Displays the timer values configured for all the ports or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTime
```

mvrp timer leaveall

Specifies the frequency with which the LeaveAll messages are communicated.

mvrp {port *chassis/slot/port***[–***port2***] | linkagg** *agg_id***[-***agg_id2***]} timer leaveall** *timer_value*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
timer_value	Specifies the value of the LeaveAll Timer in milliseconds. The valid range is 750 milliseconds to 2147483647 milliseconds.

Defaults

parameter	default
timer-value	30000 milliseconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- LeaveAll timer value must be greater than or equal to the Leave timer value. It is recommended to have the leaveall timer 15 times greater than the leave timer.
- To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 timer leaveall 30000
-> mvrp port 1/2-12 timer leaveall 30000
-> mvrp linkagg 3 timer leaveall 30000
-> mvrp linkagg 3-6 timer leaveall 30000
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp timer	Displays the timer values configured for all the ports or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
```

mvrp timer periodic-timer

Specifies the MVRP periodic-timer time interval for the dynamically registering VLANs on the switch.

mvrp {port *chassis/slot/port***[–** *port2***] | linkagg** *agg_id***[-***agg_id2***]} timer periodic-timer** *timer_value*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
timer_value	Specifies the value of the Periodic Timer in seconds. The valid range is between 1 to 2147483647 milliseconds.

Defaults

parameter	default
timer-value	*1 second*

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 timer periodic-timer 1
-> mvrp port 1/2 timer periodic-timer 1
-> mvrp linkagg 3 timer periodic-timer 1
-> mvrp linkagg 3-6 timer periodic-timer 1
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp timer	Displays the timer values configured for all the ports or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
```

mvrp periodic-transmission

Enables the periodic transmission status on a port or aggregate of ports.

mvrp {port *chassis/slot/port***[–***port2***] | linkagg** *agg_id***[-***agg_id2***]} periodic-transmission {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables periodic transmission status on a port.
disable	Disables periodic transmission status on a port.

Defaults

By default, periodic-transmission status is disabled on all the ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 periodic-transmission enable
-> mvrp port 1/2 periodic-transmission disable
-> mvrp linkagg 10 periodic-transmission enable
-> mvrp linkagg 10 periodic-transmission disable
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigPeriodicTransmissionStatus
```

mvrp restrict-vlan-registration

Restricts MVRP processing from dynamically registering the specified VLAN or VLANs on the switch.

mvrp {port *chassis/slot/port* **[–** *port2***] | linkagg** *agg_id***[-***agg_id2***]} restrict-vlan-registration vlan** *vlan_list*

no mvrp {port *chassis/slot/port* **[–** *port2***] | linkagg** *agg_id***[-***agg_id2***]} restrict-vlan-registration vlan** *vlan_list*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
vlan_list	The VLAN ID or the VLAN ID range (for example, 1-10).

Defaults

By default, MVRP dynamic VLAN registrations are not restricted.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to allow registration of dynamic VLAN IDs through MVRP processing.
- If the specified VLAN exists on the switch, the VLAN is mapped to the receiving port.
- To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 restrict-vlan-registration vlan 5
-> no mvrp port 1/2 restrict-vlan-registration vlan 5
-> mvrp linkagg 10 restrict-vlan-registration vlan 6-10
-> no mvrp port 3/1 restrict-vlan-registration vlan 6-10
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortRestrictVlanConfigTable
   alaMvrpPortRestrictRowStatus
   alaMvrpPortRestrictVlanAttributeType
   alaMvrpPortRestrictVlanID
```

mvrp restrict-vlan-advertisement

Restricts the advertisement of VLANs on a specific port or an aggregate of ports.

mvrp {port *chassis/slot/port***[–***port2***] | linkagg** *agg_id***[-***agg_id2***]} restrict-vlan-advertisement vlan** *vlan_list*

no mvrp {port *chassis/***]***slot/port***[–***port2***] | linkagg** *agg_id***[-***agg_id2***]} restrict-vlan-advertisement vlan** *vlan_list*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
vlan_list	The list of VLAN IDs or the VLAN ID range (for example, 1-10).

Defaults

By default, MVRP VLAN advertisement is not restricted.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command affects the MVRP processing only if the applicant mode is set to participant or active.
- Use the **no** form of this command to allow the propagation of VLANs.
- To use the *agg_id* parameter, the link aggregate group must be created and enabled.

Examples

```
-> mvrp port 1/2 restrict-vlan-advertisement vlan 5
-> no mvrp port 1/2 restrict-vlan-advertisement vlan 5
-> mvrp linkagg 10 restrict-vlan-advertisement vlan 6-10
-> no mvrp port 1/2 restrict-vlan-advertisement vlan 6-10
-> no mvrp port 1/1-2 restrict-vlan-advertisement vlan 6-10
```

Release History

Release 7.2.1; command introduced.

Related Commands

mvrp applicant	Configures the applicant mode of specific ports on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.
mvrp timer join	Configures the applicant mode of specific link aggregates on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortRestrictVlanConfigTable
   alaMvrpPortRestrictRowStatus
   alaMvrpPortRestrictVlanAttributeType
   alaMvrpPortRestrictVlanID
```

mvrp static-vlan-restrict

Restricts a port from becoming a member of a statically created VLAN or a range of VLANs.

mvrp {linkagg *agg_id***[-***agg_id2***] | port** *chassis/slot/port***[–***port2***]} static-vlan-restrict vlan** *vlan_list*

no mvrp {linkagg *agg_id***[-***agg_id2***] | port** *chassis/slot/port***[–***port2***]} static-vlan-restrict vlan** *vlan_list*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
vlan_list	The list of VLAN IDs or the VLAN ID range (for example, 1-10).

Defaults

By default, ports are assigned to the static VLAN based on MVRP PDU processing.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command applies only to static VLANs and does not apply to dynamic VLANs.
- Use the **no** form of this command to set the specified port and VLAN to the default value.

Examples

```
-> mvrp port 1/2 static-vlan-restrict vlan 5
-> no mvrp port 1/2 static-vlan-restrict vlan 5
-> mvrp port 1/2 static-vlan-restrict vlan 6-9
-> no mvrp port 1/2 static-vlan-restrict vlan 6-9
-> mvrp linkagg 3 static-vlan-restrict vlan 4-5
-> no mvrp linkagg 3 static-vlan-restrict aggregate vlan 4-5
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortRestrictVlanConfigTable
   alaMvrpPortRestrictRowStatus
   alaMvrpPortRestrictVlanAttributeType
   alaMvrpPortRestrictVlanID
   alaMvrpPortConfigRegistrationToStaticVlan
   alaMvrpPortConfigRegistrationToStaticVlanLearn
   alaMvrpPortConfigRegistrationToStaticVlanRestrict
```

show mvrp configuration

Displays the global configuration for MVRP.

show mvrp configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show mvrp configuration
MVRP Enabled : yes,
Maximum VLAN Limit : 256
```

output definitions

MVRP Enabled	Indicates whether MVRP is globally enabled.
Maximum VLAN Limit	The maximum number of VLANs that can be learned by MVRP in the system.

Release History

Release 7.2.1; command introduced.

Related Commands

mvrp	Enables or disables MVRP globally on the switch.
mvrp maximum-vlan	Configures the maximum number of dynamic VLANs that can be created by MVRP.

MIB Objects

```
alaMvrpGlobalStatus
alaMvrpMaxVlanLimit
```

show mvrp port

Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

show mvrp port [*chassis/slot/port***[-***port2***]] [enable | disable]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
enable	To display only the enabled ports.
disable	To display only the disabled ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show mvrp port enable

Port   Join     Leave LeaveAll Periodic  Registration  Applicant    Periodic Tx
      Timer    Timer  Timer    Timer    Mode        Mode        Status
      (msec)   (msec) (msec)   (sec)
----+--------+--------------+--------+----------+---------+------------
1/1   600    1800   30000    2       fixed       active      enabled
1/2   600    1800   30000   2         fixed     active      enabled
1/7   600    1800    30000   2         fixed        active      enabled
1/8   600    1800    30000   2         fixed        active      enabled
2/24  600    1800    30000   2         fixed        active      enabled

-> show mvrp port disable
Port   Join     Leave LeaveAll Periodic  Registration  Applicant    Periodic Tx
      Timer    Timer  Timer    Timer    Mode        Mode        Status
      (msec)   (msec) (msec)   (sec)
----+--------+--------------+--------+----------+---------+------------
1/9   600     1800  30000    2      fixed        active        enabled
1/10  600     1800  30000    2      fixed        active        enabled
2/1   600     1800  30000    2      fixed        active        enabled
2/2   600     1800  30000    2      fixed        active        enabled
….
```

```
2/24  600     1800  30000    2      fixed        active        enabled

-> show mvrp port

Port Status    Join   Leave  LeaveAll Periodic Registration  Applicant   Periodic
               Timer  Timer  Timer    Timer    Mode           Mode        Tx Status
               (msec) (msec)  (msec)   (sec)
----+---------+------+------+--------+-------+-------------+-----------+--------
1/1  disabled  600     1800  30000    2        fixed        participant  enabled
1/2  enabled   600     1800  30000    2        fixed        participant  enabled
1/3  enabled   600     1800  30000    2        fixed        active       enabled
1/4  enabled   600     1800  30000    2        fixed        active       enabled
2/24 enabled   600     1800  30000    2        fixed        active       enabled

-> show mvrp port 1/1-3

Port Status    Join   Leave  LeaveAll Periodic Registration  Applicant   Periodic
               Timer  Timer  Timer    Timer    Mode           Mode        Tx Status
               (msec) (msec)  (msec)   (sec)
----+---------+------+------+--------+-------+-------------+-----------+--------
1/1  disabled  600     1800  30000     2      fixed        participant  enabled
1/2  enabled   600     1800  30000     2      fixed        participant  enabled
1/3  enabled   600     1800  30000     2      fixed        participant  enabled

-> show mvrp port 1/1

MVRP Enabled : no,
Registrar Mode : normal,
Applicant Mode : participant,
Join Timer (msec) : 600,
Leave Timer (msec) : 1800,
LeaveAll Timer (msec) : 30000,
Periodic Timer (sec) : 1,
Periodic Tx Status : enabled

-> show mvrp port 1/1 enable

ERROR: MVRP is disabled on port 1/1
```

output definitions

Port	Displays the slot and port number.
Join Timer	Displays the value of Join Timer in milliseconds.
Leave Timer	Displays the value of the Leave Timer in milliseconds.
LeaveAll Timer	Displays the value of the LeaveAll Timer in milliseconds.
Periodic Timer	Displays the value of the Periodic Timer in seconds.
Periodic Tx Status	The transmission status of MVRP, **enable** or **disable.**

Release History

Release 7.2.1; command introduced.

Related Commands

mvrp port	Enables or disables MVRP on specific ports on the switch.
mvrp	Configures VLAN dynamic registration mode to MVRP and deletes all static configuration of previous mode along with the dynamic data.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortStatus
   alaMvrpPortConfigRegistrarMode
   alaMvrpPortConfigApplicantMode
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
   alaMvrpPortConfigPeriodicTransmissionStatus
```

show mvrp linkagg

Displays the MVRP configurations for linkaggs, including timer values, registration and applicant modes.

show mvrp linkagg [*agg_id***[-***agg_id2***]} [enabled | disabled]**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enabled	To display only the enabled ports.
disabled	To display only the disabled ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show mvrp linkagg 1-3

Port Status    Join    Leave LeaveAll Periodic  Registration Applicant  Periodic
               Timer   Timer  Timer    Timer    Mode         Mode       Tx Status
               (msec)  (msec) (msec)   (sec)
----+---------+------+------+--------+--------+------------+------------+-------
0/1  enabled  600     1800  30000    2         fixed        participant  enabled
0/2  enabled  600     1800  30000    2         fixed        participant  enabled
0/3  enabled  600     1800  30000    2         fixed        participant  enabled

-> show mvrp linkagg 1

MVRP Enabled : yes,
Registrar Mode : normal,
Applicant Mode : participant,
Join Timer (msec) : 600,
Leave Timer (msec) : 1800,
LeaveAll Timer (msec): 30000,
Periodic Timer (sec)  : 1,
Periodic Tx Status: enabled

-> show mvrp linkagg 1 disable

ERROR: MVRP is enabled on linkagg 0/1
```

Note. In the command output shown below, the MVRP status is not displayed as the command is only for enabled ports and link aggregates.

```
-> show mvrp linkagg 10 enable

Registrar Mode        : normal,
Applicant Mode        : participant,
Join Timer (msec)     : 600,
Leave Timer (msec)    : 1800,
LeaveAll Timer (msec) : 30000,
Periodic Timer (sec)  : 1,
Periodic Tx status    : disabled
```

output definitions

Port	Displays the slot/port number.
Join Timer	Displays the value of Join Timer in milliseconds.
Leave Timer	Displays the value of the Leave Timer in milliseconds.
LeaveAll Timer	Displays the value of the LeaveAll Timer in milliseconds.
Periodic Timer	Displays the value of the Periodic Timer in seconds.
Periodic Tx Status	The transmission status of MVRP, **enable** or **disable**

Release History

Release 7.2.1; command introduced.

Related Commands

mvrp port	Enables or disables MVRP on specific ports on the switch.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortStatus
   alaMvrpPortConfigRegistrarMode
   alaMvrpPortConfigApplicantMode
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
   alaMvrpPortConfigPeriodicTransmissionStatus
```

show mvrp timer

Displays the timer values configured for all the ports or a specific port.

show mvrp [port *chassis/slot/port***[–** *port2***] | linkagg** *agg_id***[-***agg_id2***]] timer {join | leave | leaveall | periodic-timer}**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
join	To display only the join timer.
leave	To display only the leave timer.
leaveall	To display only the leaveall timer.
periodic-timer	To display only the periodic-timer.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **join**, **leave**, **leaveall**, or **periodic-timer** parameter with this command to view the specific timer values configured on all the ports.
- Use the *agg_id* or *slot/port* parameter with this command to display the timer values configured for a specific port.

Examples

```
-> show mvrp timer

Port    Join Timer     Leave Timer    LeaveAll Timer   Periodic Timer
        (msec)         (msec)          (sec)             (msec)
--------+--------------+--------------+---------------+----------------
1/1      600            1800            30000             2
1/2      600            1800            30000             5
1/3      600            1800            30000             1
1/4      600            1800            30000             1

-> show mvrp port 1/21 timer

Join Timer (msec) : 600,
Leave Timer (msec) : 1800,
```

```
LeaveAll Timer (msec) : 30000,
Periodic-Timer (sec) : 1
-> show mvrp port 1/21 timer join

Join Timer (msec) : 600

-> show mvrp port 1/21 timer leave

Leave Timer (msec) : 1800

-> show mvrp port 1/21 timer leaveall

LeaveAll Timer (msec) : 30000

-> show mvrp port 1/21 timer periodic-timer

Periodic-Timer (sec) : 1

-> show mvrp timer join

Legend : All timer values are in milliseconds
Port      Join Timer
--------+----------------
1/1       600
1/2       600
1/3       600

-> show mvrp timer leaveall

Legend : All timer values are in milliseconds
Port     LeaveAll Timer
--------+----------------
1/1      1800
1/2      1800
1/3      1800

-> show mvrp timer leaveall

Legend : All timer values are in milliseconds
Port      LeaveAll Timer
--------+----------------
1/1       30000
1/2       30000
1/3       30000

-> show mvrp timer periodic-timer

Port      Periodic Timer
--------+----------------
1/1        1
1/2        1
1/3        1
```

output definitions

Port	Displays the slot/port number.
Join Timer	Displays the value of Join Timer in milliseconds.
Leave Timer	Displays the value of the Leave Timer in milliseconds.

output definitions (continued)

LeaveAll Timer	Displays the value of the LeaveAll Timer in milliseconds.
Periodic Timer	Displays the value of the Periodic Timer in seconds.

Release History

Release 7.2.1; command introduced.

Related Commands

mvrp timer join	Specifies the join time interval between transmit opportunities for the dynamically registering VLANs on the switch.
mvrp timer leave	Specifies the period of time that the switch has to wait in the Leave state before changing to the unregistered state.
mvrp timer leaveall	Specifies the frequency with which the LeaveAll messages are communicated.
mvrp timer periodic-timer	Specifies the MVRP periodic-timer time interval for the dynamically registering VLANs on the switch.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigJoinTimer
   alaMvrpPortConfigLeaveTimer
   alaMvrpPortConfigLeaveAllTimer
   alaMvrpPortConfigPeriodicTimer
```

show mvrp statistics

Displays the MVRP statistics for all the ports, aggregates, or specific ports.

show mvrp {port *chassis/slot/port***[–** *port2***] | linkagg** *agg_id***[-***agg_id2***]} statistics**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If no port or link aggregate is specified the MVRP statistics are displayed for all ports.
- Use the *agg_id* or *slot/port* parameter with this command to display the MVRP statistics for a specific port.

Examples

```
-> show mvrp port 1/21 statistics

Port 1/21
New Received   : 0,
Join In Received   : 1526,
Join Empty Received   : 8290,
Leave Received   : 0,
In Received   : 1,
Empty Received   : 0,
Leave All Received   : 283,
New Transmitted   : 826,
Join In Transmitted   : 1532,
Join Empty Transmitted   : 39,
Leave Transmitted   : 0,
In Transmitted   : 0,
Empty Transmitted   : 296,
LeaveAll Transmitted   : 23,
Failed Registrations   : 0,
Total Mrp PDU Received   : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msgs Received  : 10100,
Total Mrp Msgs Transmitted: 2693,
Invalid Msgs Received   : 0
```

```
-> show mvrp statistics

Port 1/1:
New Received   : 0,
Join In Received   : 1526,
Join Empty Received   : 8290,
Leave Received   : 0,
In Received   : 1,
Empty Received   : 0,
Leave All Received   : 283,
New Transmitted   : 826,
Join In Transmitted   : 1532,
Join Empty Transmitted   : 39,
Leave Transmitted   : 0,
In Transmitted   : 0,
Empty Transmitted   : 296,
LeaveAll Transmitted   : 23,
Failed Registrations   : 0,
Total Mrp PDU Received   : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msgs Received  : 10100,
Total Mrp Msgs Transmitted: 2693,
Invalid Msgs Received   : 0

Port 1/2:
New Received   : 0,
Join In Received   : 1526,
Join Empty Received   : 8290,
Leave Received   : 0,
In Received   : 1,
Empty Received   : 0,
Leave All Received   : 283,
New Transmitted   : 826,
Join In Transmitted   : 1532,
Join Empty Transmitted   : 39,
Leave Transmitted   : 0,
In Transmitted   : 0,
Empty Transmitted   : 296,
LeaveAll Transmitted   : 23,
Failed Registrations   : 0,
Total Mrp PDU Received   : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msgs Received  : 10100,
Total Mrp Msgs Transmitted: 2693,
Invalid Msgs Received   : 0
```

output definitions

New Received	The number of new MVRP messages received on the switch.
Join In Received	The number of MVRP Join In messages received on the switch
Join Empty Received	The number of MVRP Join Empty messages received on the switch.
Leave In Received	The number of MVRP Leave In messages received on the switch.
In Received	The total MVRP messages received on the switch.
Empty Received	The number of MVRP Empty messages received on the switch.
Leave All Received	The number of MVRP Leave All messages received on the switch.

output definitions (continued)

New Transmitted	The number of new MVRP messages sent by the switch.
Join In Transmitted	The number of MVRP Join In messages sent by the switch
Join Empty Transmitted	The number of MVRP Join Empty messages sent by the switch.
Leave Transmitted	The number of MVRP Leave messages sent by the switch.
In Transmitted	The number of MVRP In messages sent by the switch.
Empty Transmitted	The number of MVRP empty messages sent by the switch.
LeaveAll Transmitted	The number of Leave All messages sent by the switch.
Failed Registrations	The number of failed registrations.
Total Mrp PDU Received	The number of total MRP PDUs received by the switch.
Total Mrp Msgs Received	The number of total MRP messages received by the switch.
Total Mrp Msgs Transmitted	The number of total MRP messages sent by the switch.
Invalid Msgs Received	The number of invalid messages received by the switch.

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp configuration	Clears MVRP statistics for all ports, an aggregate of ports, or a specific port.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaMvrpPortStatsTable
   alaMvrpPortStatsNewReceived
   alaMvrpPortStatsJoinInReceived
   alaMvrpPortStatsJoinEmptyReceived
   alaMvrpPortStatsLeaveReceived
   alaMvrpPortStatsInReceived
   alaMvrpPortStatsEmptyReceived
   alaMvrpPortStatsLeaveAllReceived
   alaMvrpPortStatsNewTransmitted
   alaMvrpPortStatsJoinInTransmitted
   alaMvrpPortStatsJoinEmptyTransmitted
   alaMvrpPortStatsLeaveTransmitted
   alaMvrpPortStatsInTransmitted
   alaMvrpPortStatsEmptyTransmitted
   alaMvrpPortStatsLeaveAllTransmitted
   alaMvrpPortStatsTotalPDUReceived
   alaMvrpPortStatsTotalPDUTransmitted
   alaMvrpPortStatsTotalMsgsReceived
   alaMvrpPortStatsTotalMsgsTransmitted
   alaMvrpPortStatsInvalidMsgsReceived
   alaMvrpPortFailedRegistrations
```

show mvrp last-pdu-origin

Displays the source MAC address of the last MVRP message received on specific ports or aggregates.

show mvrp {port *chassis/slot/port***[–** *port2***] | linkagg** *agg_id***[-***agg_id2***]} last-pdu-origin**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show mvrp port 1/1-3 last-pdu-origin

Port     Last PDU Origin
--------+------------------
1/1      00:d0:95:ee:f4:64
1/2      00:d0:95:ee:f4:65
1/3      00:d0:95:ee:f4:66

->show mvrp port 1/21 last-pdu-origin

Port     Last PDU Origin
--------+------------------
1/1      00:d0:95:ee:f4:64
```

output definitions

Port	Displays the slot and port number.
Last PDU origin	The source MAC address of the last PDU message received on the specific port.

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp linkagg	Displays the MVRP configuration for a specific port or an aggregate of ports.
show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

```
alaMvrpPortStatsTable
   alaMvrpPortLastPduOrigin
```

show mvrp vlan-restrictions

Displays the VLAN MVRP configuration on a specific port or an aggregate of ports.

show mvrp {port *chassis/slot/port***[–** *port2***] | linkagg** *agg_id***[-***agg_id2***]} vlan-restrictions**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the *agg_id* or *slot/port* parameter with this command to display the MVRP statistics for a specific port.

Examples

```
-> show mvrp port 1/21 vlan-restrictions

VLAN ID             Static      Restricted      Restricted
                 Registration   Registration    Applicant
--------------+--------------+--------------+-----------
     1               LEARN          FALSE          FALSE
     2               LEARN          FALSE          FALSE
     3               LEARN          FALSE          FALSE
     4               LEARN          FALSE          FALSE
     5               LEARN          FALSE          FALSE
     6               LEARN          FALSE          FALSE
     7               LEARN          FALSE          FALSE
    11               RESTRICT       FALSE          FALSE
    12               RESTRICT       FALSE          FALSE
    53               LEARN          TRUE           FALSE
    55               LEARN          FALSE          TRUE
```

output definitions

VLAN ID	The VLAN identification number for a preconfigured VLAN that handles the MVRP traffic for this port.
Static Registration	Indicates if the port is restricted (**RESTRICT**) or not restricted (**LEARN**) from becoming a member of the static VLAN.

output definitions (continued)

Restricted Registration	Indicates if the VLAN is restricted (**TRUE**) or not restricted (**FALSE**) from dynamic registration on the port.
Restricted Applicant	Indicates if the VLAN is restricted for advertisement from the port (**TRUE**) or not (**FALSE**).

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp port	Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
show mvrp linkagg	Displays the MVRP configuration for a specific port or an aggregate of ports.

MIB Objects

```
alaMvrpPortConfigTable
   alaMvrpPortConfigRestrictedRegistrationBitmap
   alaMvrpPortConfigRestrictedApplicantBitmap
   alaMvrpPortConfigRegistrationToStaticVlan
```

mvrp clear-statistics

Clears MVRP statistics for all the ports, an aggregate of ports, or a specific port.

mvrp [port *chassis/slot/port* **[–***port2***] | linkagg** *agg_id***[-***agg_id2***]] clear-statistics**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

If no ports are specified, the MVRP statistics are deleted for all the ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the *agg_id* or *slot/port* parameter with this command to clear MVRP statistics for a specific port.

Examples

```
-> mvrp clear-statistics
-> mvrp port 1/2 clear-statistics
-> mvrp linkagg 10 clear-statistics
```

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp statistics	Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpGlobalClearStats
   alaMvrpPortStatsTable
   alaMvrpPortStatsClearStats
```

16 802.1AB Commands

802.1AB is an IEEE standard for exchanging information with neighboring devices and maintaining a database of it. The information is exchanged as an LLDPDU (Link Layer Discovery Protocol Data Unit) in TLV (Time, Length, Value) format. This chapter details configuring and monitoring 802.1AB on a switch.

The OmniSwitch version of 802.1AB complies with the following:

- IEEE 802.1AB-2009 Station and Media Access Control Discovery
- ANSI-TIA 1057-2006 Link Layer Discovery Protocol for Media End Point Devices.

MIB information for the 802.1AB commands is as follows:

MIB Filename: LLDP-MIB.mib, LLDP-TC-MIB.mib, LLDP-EXT-DOT1-MIB.mib, LLDP-EXT-DOT3-MIB.mib, LLDP-EXT-MED-MIB.mib

*MIB V2 Filenam*es: LLDP-V2-MIB.mib, LLDP-V2-TC-MIB.mib, LLDP-EXT-DOT1-V2-MIB.mib, LLDP-EXT-DOT3-V2-MIB.mib, LLDP-EXT-MED-MIB.mib

Filename: ALCATEL-IND1-LLDP-MED-MIB.mib
Module: alcatelIND1LLDPMEDMIB

Filename: ALCATEL-IND1-LLDP-TRUST-MIB.mib
Module: alcatelIND1LLDPTRUSTMIB

A summary of available commands is listed here:

lldp nearest-edge mode
lldp transmit interval
lldp transmit hold-multiplier
lldp reinit delay
lldp notification interval
lldp lldpdu
lldp notification
lldp network-policy
lldp med network-policy
lldp tlv management
lldp tlv dot1
lldp tlv dot3
lldp tlv med
lldp tlv proprietary
lldp tlv application
lldp tlv application priority
show lldp system-statistics
show lldp statistics
show lldp local-system
show lldp local-port
show lldp local-management-address
show lldp config
show lldp network-policy
show lldp med network-policy
show lldp remote-system
show lldp remote-system med
show lldp remote-system application-tlv
show lldp agent-destination-address
lldp trust-agent
lldp trust-agent violation-action
show lldp trusted remote-agent
show lldp trust-agent

Configuration procedures for 802.1AB are explained in “Configuring 802.1AB,” *OmniSwitch AOS Release 8 Network Configuration Guide*.

lldp nearest-edge mode

Enables or disables the nearest-edge mode for the switch. When enabled, the switch will use the LLDP destination MAC address (01:20: DA: 02:01:73) to send LLDPDUs.

lldp nearest-edge mode {enable | disable}

Syntax Definitions

enable	Enables the nearest-edge mode.
disable	Disables the nearest-edge mode.

Defaults

NA

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **nearest-edge** MAC address is used in conjunction with the Auto Download Configuration feature to advertise the management VLAN.
- This mode is used to learn the Management VLAN ID from a centralized Remote Configuration management switch.

Examples

```
-> lldp nearest-edge mode enable
```

Release History

Release 7.3.4; command introduced.

Related Commands

show lldp local-system	Displays local system information.

MIB Objects

```
lldpDestMac
```

lldp transmit interval

Sets the transmit time interval for LLDPDUs.

lldp transmit interval *seconds*

Syntax Definitions

seconds	The transmit interval between LLDPDUs, in seconds. The valid range is 5 - 32768.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The LLDP protocol must be enabled before using this command.

Examples

```
-> lldp transmit interval 40
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp transmit hold-multiplier	Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpV2MessageTxInterval
```

lldp transmit hold-multiplier

Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.

lldp transmit hold-multiplier *num*

Syntax Definitions

num	The transmit hold multiplier value. The valid range is 2-10.

Defaults

parameter	default
num	4

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LLDP protocol must be enabled before using this command.
- The Time To Live is a multiple of transmit interval and transmit hold multiplier.

Examples

```
-> lldp transmit hold-multiplier 6
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp transmit interval	Sets the transmit time interval for LLDPDUs.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpV2MessageTxHoldMultiplier
```

lldp reinit delay

Sets the time interval that must elapse before the current status of a port is reinitialized after a status change.

lldp reinit delay *seconds*

Syntax Definitions

seconds	The number of seconds to reinitialize the ports status after a status change. The valid range is 1-10.

Defaults

parameter	default
seconds	2

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The LLDP protocol must be enabled before using this command.

Examples

```
-> lldp reinit delay 4
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp transmit interval	Sets the minimum time interval between successive LLDPDUs transmitted.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpV2ReinitDelay
```

lldp notification interval

Sets the time interval that must elapse before a notification about the local system MIB change is generated.

lldp notification interval *seconds*

Syntax Definitions

seconds	The minimum number of seconds for generating a notification-event. The valid range is 5-3600.

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LLDP protocol and notification must be enabled before using this command.
- In a specified interval, it is not possible to generate more than one notification-event.

Examples

```
-> lldp notification interval 25
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp notification	Specifies the switch to control per port notification status about the remote device change.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpV2NotificationInterval
```

lldp lldpdu

Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port *chassis/slot/port***[-***port2***] | slot** *chassis/slot* | **chassis} lldpdu {tx | rx | tx-and-rx | disable}**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
all	All LLDP agents.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
chassis	Specifies the whole chassis.
tx	Transmits LLDPDUs.
rx	Receives LLDPDUs.
tx-and-rx	Transmits and receives LLDPDUs.
disable	Disables LLDPDUs transmission and reception.

Defaults

parameter	default
tx | rx | tx-and-rx | disable	**tx-and-rx**
non-tpmr | nearest-customer | nearest-bridge	**nearest-bridge**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The port can be set to receive, transmit, or transmit and receive LLDPDUs using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.

- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp port 1/2 lldpdu tx-and-rx
-> lldp slot 3 lldpdu tx
-> lldp chassis lldpdu disable
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
lldp notification	Specifies the switch to control per port notification status about the remote device change.

MIB Objects

```
lldpV2PortConfigTable
   lldpV2PortConfigIfIndex
   lldpV2PortConfigDestAddressIndex
   lldpV2PortConfigAdminStatus
```

lldp notification

Specifies the switch to control per port notification status about the remote device change.

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port *chassis/slot/port***[-***port2***] | slot** *chassis/slot* | **chassis} notification {enable | disable}**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
all	All LLDP agents.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
chassis	Specifies the whole chassis.
enable	Enables the notification of local system MIB changes.
disable	Disables the notification.

Defaults

parameter	default
enable | disable	**disable**
non-tpmr | nearest-customer | nearest-bridge	**nearest-bridge**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LLDPDU administrative status must be in the receive state before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.

- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp port 1/2 notification enable
-> lldp slot 1 notification disable
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp notification interval	Sets the time interval that must elapse before a notification about the local system MIB change is generated.
lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

MIB Objects

```
lldpPortConfigTable
   lldpV2PortConfigPortNum
   lldpV2PortConfigDestAddressIndex
   lldpV2PortConfigNotificationEnable
```

lldp network-policy

Configures a local Network Policy on the switch for a specific application type.

lldp network-policy *policy_id* **application {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} vlan {untagged | priority-tag |** *vlan-id***} [l2-priority** *802.1p_value***] [dscp** *dscp_value***]**

no lldp network-policy *policy_id* - [*policy_id2*]

Syntax Definitions

policy_id -[*policy_id2*]	A network policy identifier (0-31) which is associated to a port. Supported only with the **no** form of the command
voice	Specifies a voice application type.
voice-signaling	Specifies a voice-signaling application type.
guest-voice	Specifies a guest-voice application type.
guest-voice-signaling	Specifies a guest-voice-signaling application type.
softphone-voice	Specifies a softphone-voice application type.
video-conferencing	Specifies a video-conferencing application type.
streaming-video	Specifies a streaming-video application type.
video-signaling	Specifies a video-signaling application type.
untagged	Specifies that a VLAN port is untagged.
priority-tag	Specifies the internal priority that would be assigned to the VLAN**.**
vlan_id	VLAN identifier. Valid range is 1–4094.
802.1p_value	The Layer-2 priority value assigned to the VLAN. Valid range is 0–7.
dscp_value	Priority value assigned to the DSCP (Differentiated Service Code Point) header. Valid range is 0–63.

Defaults

parameter	default
802.1p_value **for voice application**	**5**
802.1p_value **for other applications**	**0**
dscp_value	**0**

By default, the VLAN ID is configured in the voice network profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the configured network policy from the system.
- When a network policy is deleted, all the associated values and port bindings are also deleted.
- A maximum of 32 network policies can be configured on a single VLAN.
- Once a policy is created, the application type, VLAN ID, 802.1p, and DSCP values can be modified.
- If a network policy ID is bound to a port, it cannot be modified.
- Use a hyphen to specify a range of Policy IDs and a space to separate multiple Policy IDs in the command.
- The range for Policy IDs is supported only with the **no** form of this command.

Examples

```
-> lldp network-policy 10 application voice vlan 20
-> lldp network-policy 11 application guest-voice-signaling vlan untagged l2–
priority 3
-> lldp network-policy 20 application voice vlan priority-tag dscp 39
-> lldp network-policy 20 application voice-signaling vlan 23 l2-priority 2 dscp 43
-> no lldp network-policy 10

-> no lldp network-policy 10-20
```

Release History

Release 8.1.1; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
show lldp network-policy	Displays the network policy details for a given policy ID.
show lldp med network-policy	Displays the network policy configured on a slot or port.

MIB Objects

```
alaLldpXMedLocMediaPolicyTable
   alaLldpXMedLocMediaPolicyId
   alaLldpXMedLocMediaPolicyAppType
   alaLldpXMedLocMediaPolicyVlanType
   alaLldpXMedLocMediaPolicyVlanID
   alaLldpXMedLocMediaPolicyPriority
   alaLldpXMedLocMediaPolicyDscp
   alaLldpXMedLocMediaPolicyUnknown
   alaLldpXMedLocMediaPolicyTagged
   alaLldpXMedLocMediaPolicyRowStatus
```

lldp med network-policy

Associates an existing network policy per LLDP agent per port, slot, or chassis. Also specifies the LLDP destination MAC address sent in LLDPDUs.

lldp [nearest-bridge | nearest-customer | non-tpmr | all] {port *chassis/slot/port* **| slot** *chassis/slot* | **chassis} med network-policy** *policy_id* - [*policy_id2*]

no lldp {port *chassis/slot/port* **| slot** *chassis/slot* | **chassis} med network-policy** *policy_id* - [*policy_id2*]

Syntax Definition

nearest-bridge	Specifies the destination MAC address as 01:80:C2:00:00:0E.
nearest-customer	Specifies the destination MAC address as 01:80:C2:00:00:00.
non-tpmr	Specifies the destination MAC address as 01:80:C2:00:00:03.
all	Specifies that all three LLDP agents must be supported.
*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
chassis/slot	The chassis ID and slot number for a specific module (3/1).
chassis	Specifies all switch ports.
policy_id - [*policy_id2*]	A network policy identifier (0–31).

Defaults

NA

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disassociate a network policy from a port.
- The network policy must already be configured in the system before associating it with a port.
- A maximum of 8 network policies can be associated to a port.
- Two or more network policy IDs with the same application type cannot be associated to a port.

Examples

```
-> lldp chassis med network-policy 22
-> lldp slot 1/1 med network-policy 1-4 5 6
-> lldp por 2/1/3 med network-policy 12
-> no lldp slot 2/3 med network-policy 12
```

Release History

Release 8.1.1; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
show lldp network-policy	Displays the MED Network Policy details for a given policy ID.
show lldp med network-policy	Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

MIB Objects

```
alaLldpXMedLocMediaPolicyPortTable
   alaLldpXMedLocMediaPolicyPortIfIndex
   alaLldpXMedLocMediaPolicyId
   alaLldpXMedLocMediaPolicyPortRowStatus
```

lldp tlv management

Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port *chassis/slot/port***[-***port2***] | slot** *chassis/slot* | **chassis} tlv management {port-description | system-name | system-description | system-capabilities | management-address} {enable | disable}**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
all	All LLDP agents.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
chassis	Specifies the whole chassis.
port-description	Enables or disables the transmission of port description TLV in LLDPDU.
system-name	Enables or disables the transmission of system name TLV in LLDPDU.
system-description	Enables or disables transmission of system description TLV in LLDPDU.
system-capabilities	Enables or disables transmission of system capabilities TLV in LLDPDU.
management-address	Enables or disables transmission of management address on per port.
enable	Enables management TLV LLDPDU transmission.
disable	Disables management TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**
non-tpmr | nearest-customer | nearest-bridge	**nearest-bridge**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp port 1/2 tlv management port-description enable
-> lldp slot 2 tlv management management-address enable
-> lldp slot 3 tlv management system-name disable
-> lldp chassis tlv management system-capabilities enable
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
show lldp local-system	Displays local system information.
show lldp local-port	Displays per port information.
show lldp remote-system	Displays per local port and information of remote system.

MIB Objects

```
lldpV2PortConfigTable
   lldpV2LocPortPortNum
   lldpV2PortConfigTLVsTxEnable
lldpV2ConfigManAddrTable
   lldpV2ConfigManAddrPortsTxEnable
```

lldp tlv dot1

Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port *chassis/slot/port***[-***port2***] | slot** *chassis/slot* | **chassis} tlv dot1 {port-vlan | vlan-name} {enable | disable}**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
all	All LLDP agents.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
chassis	Specifies the whole chassis.
port-vlan	Enables or disables transmission of port VLAN TLV in LLDPDU.
vlan-name	Enables or disables transmission of VLAN name TLV in LLDPDU.
enable	Enables 802.1 TLV LLDPDU transmission.
disable	Disables 802.1 TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**
non-tpmr | nearest-customer | nearest-bridge	**nearest-bridge**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- If one TLV is included then the other TLV is automatically included when you use this command.

- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp port 5/1 tlv dot1 port-vlan enable
-> lldp slot 3 tlv dot1 vlan-name enable
-> lldp slot 3 tlv dot1 vlan-name disable
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
show lldp statistics	Displays per port statistics.
show lldp local-port	Displays per port information.

MIB Objects

```
lldpV2PortConfigTable
   lldpV2PortConfigPortNum
lldpV2Xdot1ConfigPortVlanTable
   lldpV2Xdot1ConfigPortVlanTxEnable
lldpV2Xdot1ConfigVlanNameTable
   lldpV2Xdot1ConfigVlanNameTxEnable
```

lldp tlv dot3

Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port *chassis/slot/port* **[-***port2***]| slot** *chassis/slot* | **chassis} tlv dot3 mac-phy {enable | disable}**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
all	All LLDP agents.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
chassis	Specifies the whole chassis.
enable	Enables 802.3 TLV LLDPDU transmission.
disable	Disables 802.3 TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**
non-tpmr | nearest-customer | nearest-bridge	**nearest-bridge**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.

- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp port 2/4 tlv dot3 mac-phy enable
-> lldp slot 2 tlv dot3 mac-phy disable
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot1	Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.
show lldp statistics	Displays per port statistics.

MIB Objects

```
lldpV2PortConfigTable
   lldpV2PortConfigPortNum
lldpV2Xdot3PortConfigTable
   lldpV2Xdot3PortConfigTLVsTxEnable
```

lldp tlv med

Specifies the switch to control per port LLDP-MED (Media Endpoint Device) TLVs to be incorporated in the LLDPDUs.

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port *chassis/slot/port* **[-***port2***] | slot** *chassis/slot* | **chassis} tlv med {power | capability} {enable | disable}**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
all	All LLDP agents.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
chassis	Specifies the whole chassis.
capability	Enables or disables transmission of LLDP-MED capabilities TLV in LLDPDU.
enable	Enables LLDP-MED TLV LLDPDU transmission.
disable	Disables LLDP-MED TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**
non-tpmr | nearest-customer | nearest-bridge	**nearest-bridge**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command will be lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.

- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp 4/4 tlv med power enable
-> lldp 4/3 tlv med capability enable
-> lldp 4 tlv med power disable
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot1	Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.
lldp tlv dot3	Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.

MIB Objects

```
lldpV2PortConfigTable
   lldpV2PortConfigPortNum
lldpV2XMedPortConfigTable
   lldpV2XMedPortConfigTLVsTxEnable
```

lldp tlv proprietary

Allows the switch to advertise the Access Point location through the proprietary TLVs.

lldp {port *chassis/slot/port* **[-***port2***]| slot** *chassis/slot* | **chassis} tlv proprietary {enable | disable}**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
chassis	All switch ports.
enable	Enables proprietary TLVs to advertise AP location.
disable	Disables proprietary TLVs to advertise AP location.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The VLAN information is advertised through 802.1x TLV (i.e, Management VLAN is advertised if the port is a 802.1x port else default VLAN of the port is advertised). The AP location is advertised through proprietary TLV.
- If an AP is detected and authenticated on a 802.1x port, LLDP TLVs are triggered to advertise management VLAN and AP location despite CLI configuration being disabled.
- If an AP is removed from 802.1x port, LLDP receives message from 802.1x port after which LLDP stops advertising of management VLAN and AP location, only if the configuration is disabled explicitly on the port.

Examples

```
-> lldp port 5/1 tlv proprietary enable
-> lldp port 5/1 tlv proprietary disable
-> lldp slot 2 tlv proprietary enable
-> lldp slot 2 tlv proprietary disable
-> lldp chassis tlv proprietary enable
-> lldp chassis tlv proprietary disable
```

Release History

Release 8.4.1.R02; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
show lldp statistics	Displays per port statistics.
show lldp local-port	Displays per port information.

MIB Objects

```
alaLldpPropConfigTable
   alaLldpPropAPLocation
```

lldp tlv application

Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port. This TLV is only configurable for the nearest-bridge LLDP agent.

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port *chassis/slot/port* **[-***port2***]| slot** *chassis/slot* | **chassis} tlv application {enable | disable}**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
all	All LLDP agents.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
chassis	Specifies the whole chassis.
enable	Enables Application Priority TLV LLDPDU transmission.
disable	Disables Application Priority TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**
non-tpmr | nearest-customer | nearest-bridge	**nearest-bridge**

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.

- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp port 2/4 tlv application enable
-> lldp slot 2 tlv application disable
```

Release History

Release 7.3.2; command introduced.

Related Commands

lldp tlv application priority	Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.
show lldp config	Displays per port statistics.

MIB Objects

```
lldpXdot1dcbxConfigApplicationPriorityTable
   lldpXdot1dcbxConfigApplicationPriorityTxEnable
```

lldp tlv application priority

Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port *chassis/slot/port***[-***port2***] | slot** *chassis/slot* | **chassis} tlv application {fcoe | iscsi | ethertype** *etype* **| tcp-sctp-port** *protocol* **| udp-dccp-port** *protocol* | **port** *protocol***} priority** *priority*

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
all	All LLDP agents.
chassis	The chassis identifier when running in virtual chassis mode.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
chassis	Specifies the whole chassis.
fcoe	Advertise the specified priority value to use for FCoE traffic.
iscsi	Advertise the specified priority value to use for SCSI traffic.
etype	Advertise the specified priority value to use for this Ethertype.
protocol	Advertise the specified priority value to use for the specified protocol.

Defaults

parameter	default
enable | disable	**disable**
non-tpmr | nearest-customer | nearest-bridge	**nearest-bridge**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LLDPDU must be enabled and set to transmit and receive before using this command.
- The Application Priority TLV must be enabled for transmission.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.

- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp port 1/1/3 tlv application fcoe priority 3
-> lldp port 1/1/3 tlv application tcp-sctp-port 3192 priority 5
```

Release History

Release 7.3.2; command introduced.

Related Commands

lldp tlv application	Enables or disables Application Priority TLV in LLDPDUs.
show lldp config	Displays the LLDP port configuration.

MIB Objects

```
alaXdot1dcbxAdminApplicationPriorityAppTable
   alaXdot1dcbxAdminApplicationPriorityAEPriority
```

show lldp system-statistics

Displays system-wide statistics.

show lldp system-statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show lldp system-statistics
 Local LLDP Agent System Statistics:
  Remote Systems Last Change  = 0 days 0 hours 3 minutes and 10 seconds,
  Remote Systems MIB Inserts  = 2,
  Remote Systems MIB Deletes  = 0,
  Remote Systems MIB Drops    = 0,
  Remote Systems MIB Age Outs = 0
```

output definitions

Remote Systems Last Change	The last change recorded in the tables associated with the remote system.
Remote Systems MIB Inserts	The total number of complete inserts in the tables associated with the remote system.
Remote Systems MIB Deletes	The total number of complete deletes in tables associated with the remote system.
Remote Systems MIB Drops	The total number of LLDPDUs dropped because of insufficient resources.
Remote Systems MIB Age Outs	The total number of complete age-outs in the tables associated with the remote system.

Release History

Release 7.1.1; command introduced.

Related Commands

lldp notification	Specifies the switch to control per port notification status about the remote device change.
lldp notification interval	Sets the time interval that must elapse before a notification about the local system MIB change is generated.

MIB Objects

```
lldpStatistics
   lldpStatsRemTablesLastChangeTime
   lldpStatsRemTablesInserts
   lldpStatsRemTablesDeletes
   lldpStatsRemTablesDrops
   lldpStatsRemTablesAgeouts
```

show lldp statistics

Displays per port statistics.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port *chassis/slot/port* **[-***port2***] slot** *chassis/slot***] statistics**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.

Defaults

By default, statistics for all LLDP ports are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the *slot/port* option is not specified, statistics for the chassis are displayed.
- If the statistics are zero they are not displayed.

Examples

```
-> show lldp statistics
           LLDPDU    LLDPDU   LLDPDU    LLDPDU   LLDPDU     TLV      TLV       Device
Slot/Port    Tx     TxLenErr    Rx      Errors   Discards  Unknown  Discards   Ageouts
---------+---------+---------+---------+---------+---------+---------+---------+--------
   1/1        453        0       452         0         0         0         0       0
   1/2        452        0       453         0         0         0         0       0
   1/5        452        0       473         0         0       476       476       0
   1/8        455        0       464         0         0         0         0       0
   1/9        456        0       464         0         0         0         0       0
  1/10        454        0       464         0         0         0         0       0
  1/11        453        0       447         0         0         0         0       0
  1/12        453        0         0         0         0         0         0       0
  1/13        453        0         0         0         0         0         0       0
  1/14        453        0         0         0         0         0         0       0
  1/17        453        0       963         0         0       449       449       0
  1/18        453        0         0         0         0         0         0       0
   2/1        452        0       457         0         0         0         0       0
```

```
2/2         452         0         963         0         0         0         0         0
2/3         480         0         459         0         0         0         0         2
```

output definitions

Slot/Port	Slot number for the module and physical port number on that module.
LLDPDU Tx	The total number of LLDPDUs transmitted on the port.
LLDPDU Rx	The total number of valid LLDPDUs received on the port.
LLDPDU Errors	The total number of invalid LLDPDUs discarded on the port.
LLDPDU Discards	The total number of LLDPDUs discarded on the port.
TLV Unknown	The total number of unrecognized LLDP TLVs on the port.
TLV Discards	The total number of LLDP TLVs discarded on the port.
Device Ageouts	The total number of complete age-outs on the port.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

MIB Objects

```
lldpV2StatsTxPortTable
   lldpV2StatsTxPortNum
   lldpV2StatsTxPortFramesTotal
lldpV2StatsRxPortTable
   lldpV2StatsRxPortNum
   lldpV2StatsRxPortFramesDiscardedTotal
   lldpV2StatsRxPortFramesErrors
   lldpV2StatsRxPortFramesTotal
   lldpV2StatsRxPortTLVsDiscardedTotal
   lldpV2StatsRxPortTLVsUnrecognizedTotal
   lldpV2StatsRxPortAgeoutsTotal
```

show lldp local-system

Displays local system information.

show lldp local-system

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show lldp local-system
Local LLDP Agent System Data:
  Chassis ID Subtype          = 4 (MAC Address),
  Chassis ID                  = 00:d0:95:e9:c9:2e,
  System Name                 = OS6900-DC1,
  System Description          = 7.3.2.315.R01 Development, June 03, 2013.,
  Capabilites Supported       = Bridge, Router,
  Capabilites Enabled         = Bridge, Router,
  LLDPDU Transmit Interval    = 30 seconds,
  TTL Hold Multiplier         = 4,
  LLDPDU Transmit Delay       = 2 seconds,
  Reintialization Delay       = 2 seconds,
  MIB Notification Interval   = 5 seconds
  Management Address Type     = 1 (IPv4),
  Management IP Address       = 10.255.11.100,
```

output definitions

Chassis ID Subtype	The subtype that describe chassis ID.
Chassis ID	The chassis ID (MAC address).
System Name	The name of the system.
System Description	The description of the system.
Capabilites Supported	The capabilities of the system.
Capabilites Enabled	The enabled capabilities of the system.
LLDPDU Transmit Interval	The LLDPDU transmit interval.
TTL Hold Multiplier	The hold multiplier used to calculate TTL.

output definitions (continued)

LLDPDU Transmit Delay	The minimum transmit time between successive LLDPDUs.
Reintialization Delay	The minimum time interval before the reinitialization of local port objects between port status changes.
MIB Notification Interval	The minimum time interval between consecutive notifications of local system MIB change.
Management Address Type	The type of management address used in LLDPDU.
Management IP Address	The management IP address. The loopback0 IP address is configured for the management IP address to be transmitted.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp reinit delay	Sets the time interval that must elapse before the current status of a port is reinitialized after a status change.
lldp transmit hold-multiplier	Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.
lldp transmit interval	Sets the minimum time interval between successive LLDPDUs transmitted.

MIB Objects

```
lldpV2LocalSystemData
   lldpV2LocChassisIdSubtype
   lldpV2LocChassisId
   lldpV2LocSysName
   lldpV2LocSysDesc
   lldpV2LocSysCapSupported
   lldpV2LocSysEnabled
lldpV2PortConfigTable
   lldpV2MessageTxInterval
   lldpV2MessageTXHoldMultiplier
   lldpV2TxDelay
   lldpV2ReinitDelay
   lldpV2NotificationInterval
lldpV2LocManAddrTable
   lldpV2LocManAddrSubtype
   lldpV2LocManAddr
```

show lldp local-port

Displays per port information.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port *chassis/slot/port* **[-***port2***]| slot** *chassis/slot***] local-port**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.

Defaults

By default, a list of all LLDP ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show lldp local-port
Local Port 1/1/1 LLDP Info:
  Port ID                     = 1001 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 XNI 1/1/1,
  Vlan                        = 1,
  AP Location                 = sw1,
Local Port 1/1/2 LLDP Info:
  Port ID                     = 1002 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 XNI 1/1/2,
  Vlan                        = 1,
  AP Location                 = -,
Local Port 1/1/3 LLDP Info:
  Port ID                     = 1003 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 GNI 1/1/3,
  Vlan                        = 1,
  AP Location                 = -,
Local Port 1/1/4 LLDP Info:
  Port ID                     = 1004 (Locally assigned),
```

```
  Port Description            = Alcatel-Lucent OS6865 GNI 1/1/4,
  Vlan                        = 1,
  AP Location                 = -,
Local Port 1/1/5 LLDP Info:
  Port ID                     = 1005 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 GNI 1/1/5,
  Vlan                        = 1,
  AP Location                 = -,
Local Port 1/1/6 LLDP Info:
  Port ID                     = 1006 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 GNI 1/1/6,
   Vlan                        = 4095,
  AP Location                 = -,
Local Port 1/1/7 LLDP Info:
  Port ID                     = 1007 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 GNI 1/1/7,
   Vlan                        = 1,
  AP Location                 = -,
Local Port 1/1/8 LLDP Info:
  Port ID                     = 1008 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 GNI 1/1/8,
   Vlan                        = 1,
  AP Location                 = -,
Local Port 1/1/9 LLDP Info:
  Port ID                     = 1009 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 GNI 1/1/9,
   Vlan                        = 4095,
  AP Location                 = -,
Local Port 1/1/10 LLDP Info:
  Port ID                     = 1010 (Locally assigned),
  Port Description            = Alcatel-Lucent OS6865 GNI 1/1/10,
   Vlan                        = 4095,
  AP Location                 = -,
```

output definitions

Port ID	The port ID (port MAC).
Port Description	The description of the port (which includes the port number and the AOS version).
Vlan	Displays the authenticated VLAN (management VLAN) if AP is connected on a dot1x enabled port, else the default VLAN of the port is displayed.
AP Location	Displays the location to which the AP is connected.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
Release 8.4.1.R02; **Vlan** and **AP Location** output fields added.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot1	Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.
lldp tlv proprietary	Allows the switch to advertise the Access Point location through the proprietary TLVs.

MIB Objects

```
lldpV2LocPortTable
   lldpV2LocPortNum
   lldpV2LocPortIdsubtype
   lldpV2LocPortId
   lldpV2LocPortDesc
   alaLldpPropAPLocation
   alaLldpPropVlan
   alaLldpPropLocationDesc
```

show lldp local-management-address

Displays the local management address information.

show lldp local-management-address

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show lldp local-management-address
Local LLDP Agent Management Address:
  Management Address Type     = 1 (IPv4),
  Management IP Address       = 10.255.11.100
```

output definitions

Management Address Type	The address type used to define the interface number (IPv4 or IPv6).
Management IP Address	The management IP address. The loopback0 IP address is configured for the management IP address to be transmitted.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpV2LocManAddrTable
   lldpV2LocManAddrLen
   lldpV2LocManAddrIfSubtype
   lldpV2LocManAddrIfId
```

show lldp config

Displays the general LLDP configuration information for LLDP ports.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port *chassis/***]***slot/port* **[-***port2***] | slot** *chassis/slot***] config [application-tlv]**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
application-tlv	Displays Application Priority TLV parameters.

Defaults

By default, a list of all LLDP ports with their configuration parameters is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the *slot/port* or *slot* parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp config
----------+-----------------------------------------+--------------------+---------+--------------
          |  Admin    |  Notify  |  Std TLV |   Mgmt   |  802.1   |  802.3   |   MED   |  Proprietary
 Slot/Port|  Status   |   Trap   |   Mask   | Address  |   TLV    |   Mask   |   Mask  |      TLV
----------+-----------+----------+----------+----------+----------+----------+---------+--------------
   1/1      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/2      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/3      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/4      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/5      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/6      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/7      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/8      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/9      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
   1/10     Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00       0x00      Disabled
```

```
-> show lldp config application-tlv
Slot/
 Port   Selector                       Protocol     Priority
------+------------------------------+-----------+------------+
  1/2   Ethertype                       0x8906        3
  1/2   Tcp/Sctp                       3260          4
  1/20  Tcp/Sctp                       3190          3
  1/20  Udp/Dccp                        300           4
  1/20  Tcp/Udp/Sctp/Dccp               300           4
```

output definitions

Slot/Port	The LLDP slot and port number.
Admin Status	Indicates the Administrative status of the LLDP port. The options are: **Disabled**, **Rx**, **Tx**, and **Rx+Tx**.
Notify Trap	Indicates whether the Notify Trap feature is disabled or enabled on a particular port.
Std TLV Mask	The standard TLV mask set for the port.
Mgmt Address	Indicates whether transmission of the per port IPv4 management address is enabled or disabled.
802.1 TLV	Indicates whether 802.1 TLV status is enabled or disabled on the LLDP port.
802.3 Mask	The standard 802.3 mask set for the port.
MED Mask	The standard MED mask set for the port.
App-Prio TLV	Indicates the Application priority TLV status.
Trust Status	Indicates the Trust Status.
Proprietary TLV	Indicates the proprietary TLV status.

Release History

Release 7.1.1; command introduced.
Release 7.3.2; **App-Prio TLV** field added, **application-tlv** parameter added.
Release 7.3.1; Version 2 (2009) updates implemented.
Release 8.4.1.R02; **Proprietary TLV** output field added.

Related Commands

lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
lldp notification	Specifies the switch to control per port notification status about the remote device change.
lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot3	Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.
lldp tlv application	Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port.
lldp tlv application priority	Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

MIB Objects

```
lldpV2PortConfigTable
   lldpV2PortConfigPortNum
   lldpV2PortConfigAdminStatus
   lldpV2PortConfigNotificationEnable
   lldpV2LocPortPortNum
   lldpV2PortConfigTLVsTxEnable
lldpV2ConfigManAddrTable
   lldpV2ConfigManAddrPortsTxEnable
lldpV2Xdot3PortConfigTable
   lldpV2Xdot3PortConfigTLVsTxEnable
lldpV2Xdot1dcbxConfigApplicationPriorityTable
   lldpV2Xdot1dcbxConfigApplicationPriorityTxEnable
alaXdot1dcbxAdminApplicationPriorityAppTable
   alaXdot1dcbxAdminApplicationPriorityAEPriority
```

show lldp network-policy

Displays the MED Network Policy details for a given policy ID.

show lldp network-policy [*policy_id***]**

Syntax Definitions

policy_id	Policy identifier for a network policy definition. Valid range is between 0 and 31.

Defaults

By default, all configured policies are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Network policy must be configured on the system before using this command.
- Enter a policy ID with this command to display information for a specific policy.

Examples

```
-> show lldp network-policy
Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Network         Application       Vlan    Layer2   DSCP
Policy ID        Type              Id    Priority  Value
-----------+---------------------+------+--------+-------
     1      voice                  4000   7        33
    12      guest-voice               -   -        44
    21      streaming-voice           0   4        11
    31      guest-voice-signaling    23   2        1

-> show lldp network-policy 21
Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Network         Application       Vlan    Layer2   DSCP
Policy ID        Type              Id    Priority  Value
-----------+---------------------+------+--------+-------
    21      streaming-voice           0   4        11
```

output definitions

Network Policy ID	Policy identifier for a network policy definition.
Application Type	Indicates the type of application configured on the port or VLAN.
VLAN ID	The VLAN ID assigned to the port on which the network policy is configured.

output definitions

Layer2 Priority	Layer 2 priority to be used for the specified application type.
DSCP Value	DSCP value to be used to provide Diffserv node behavior for the specified application type.

Release History

Release 8.1.1 command introduced.

Related Commands

lldp network-policy	Configures a local network policy on a switch for an application type.

MIB Objects

```
alaLldpXMedLocMediaPolicyTable
   alaLldpXMedLocMediaPolicyId
   alaLldpXMedLocMediaPolicyAppType
   alaLldpXMedLocMediaPolicyVlanType
   alaLldpXMedLocMediaPolicyVlanId
   alaLldpXMedLocMediaPolicyPriority
   alaLldpXMedLocMediaPolicyDscp
   alaLldpXMedLocMediaPolicyUnknown
   alaLldpXMedLocMediaPolicyTagged
```

show lldp med network-policy

Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

show lldp [nearest-bridge | nearest-customer | non-tpmr | all] [slot *chassis/slot*| **port** *chassis/slot/port***] med network-policy**

Syntax Definitions

nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
all	Specifies that all three LLDP agents must be supported.
chassis/slot	The chassis ID and slot number for a specific module (3/1).
*chassis/slot/port***[***-port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).

Defaults

By default, all ports with associated policies are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Network policy must be configured on the system before using this command.
- Enter a slot or slot/port number with this command to display information for a specific slot or port.

Examples

```
-> show lldp slot 1/1 med network-policy

 chassis/slot/port     Network Policy ID
-------------+------------------------
    1/1/1                1 3 5 7 21 23 30 31
    1/1/2                1 2 3 4 7 8 9 10
    .
    .
    .
```

output definitions

Chassis/Slot/Port	Slot number for the module and physical port number on that module.
Network Policy ID	Policy identifier for a network policy definition.

Release History

Release 8.1.1; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
lldp med network-policy	Configures a local network policy on a switch for an application type.

MIB Objects

```
alaLldpXMedLocMediaPolicyPortTable
   alaLldpXMedLocMediaPolicyPortIfIndex
   alaLldpXMedLocMediaPolicyId
```

show lldp remote-system

Displays per local port and information of remote system.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port *chassis/slot/port* **[-***port2***] | slot** *chassis/slot***] remote-system**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.

Defaults

By default, a list of all lldp ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show lldp remote-system
Remote LLDP Agents on Local Slot/Port: 2/47,
  Chassis ID Subtype          = 4 (MAC Address),
  Chassis ID                  = 00:d0:95:e9:c9:2e,
  Port ID Subtype             = 7 (Locally assigned),
  Port ID                     = 2048,
  Port Description            = (null),
  System Name                 = (null),
  System Description          = (null),
  Capabilites Supported       = none supported,
  Capabilites Enabled         = none enabled,

Remote LLDP Agents on Local Slot/Port: 2/48,
  Chassis ID Subtype          = 4 (MAC Address),
  Chassis ID                  = 00:d0:95:e9:c9:2e,
  Port ID Subtype             = 7 (Locally assigned),
  Port ID                     = 2047,
  Port Description            = (null),
```

```
System Name                 = (null),
System Description          = (null),
Capabilites Supported       = none supported,
Capabilites Enabled         = none enabled,
```

output definitions

Remote LLDP Agents on Local Slot/Port	The Slot number to which the remote system entry is associated and the physical port number on that module.
Chassis ID Subtype	The sub type that describes chassis ID.
Chassis ID	The chassis ID (MAC address).
Port ID Subtype	The sub type that describes port ID
Port ID	The port ID (Port MAC).
Port Description	The description of the port (which includes the port number and the AOS version).
System Name	The name of the system.
System Description	The description of the system.
Capabilites Supported	The capabilities of the system.
Capabilites Enabled	The enabled capabilities of the system.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

show lldp local-port	Displays per port information.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpV2RemTable
   lldpV2RemLocalPortNum
   lldpV2RemChassisIdSubtype
   lldpV2RemChassisId
   lldpV2RemPortIdSubtype
   lldpV2RemPortId
   lldpV2RemPortDesc
   lldpV2RemSysName
   lldpV2RemSysDesc
   lldpV2RemSysCapSupported
   lldpV2RemSysCapEnabled
   lldpV2RemManAddrIfSubtype
   lldpV2RemManAddrIfId
```

show lldp remote-system med

Displays remote system MED information for a single port or all ports on a slot.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port *chassis/slot/port* **[-***port2***] | slot** *chassis/slot***] remote-system med {network-policy | inventory}**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.
network-policy	Display network-policy TLVs from remote Endpoint Devices.
inventory	Display inventory management TLVs from remote Endpoint Devices.

Defaults

By default, a list of all LLDP ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the *slot/port* or *slot* parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp port 2/47 remote-system med network-policy
Slot/  Remote   Application      Unknown    Tagged    Vlan     Layer2   DSCP
Port    ID         Type         Policy Flag Flag       Id     Priority  Value
------+------+---------------+----------+---------+------+----------+------
 1/22   1        Voice(01)         Defined  Untagged   345       4        34
 1/22   2        Guest Voice(4)    Defined  Untagged    50       3        46
```

output definitions

Slot/Port	The Slot number to which the remote system entry is associated and the physical port number on that module.
Remote ID	The Index of the Remote Device.

output definitions (continued)

Application Type	The Application type of the peer entity. 1. Voice 2. Voice Signaling 3. Guest Voice 4. Guest Voice Signaling 5. Softphone Voice 6. Video Conferencing 7. Streaming Video 8. Video Signaling
Unknown Policy Flag	Whether the network policy for the specified application type is currently defined or unknown.
Tagged Flag	Whether the specified application type is using a **tagged** or an **untagged** VLAN.
VLAN ID	The VLAN identifier (VID) for the port.
Layer 2 Priority	Layer 2 priority to be used for the specified application type.
DSCP Value	DSCP value to be used to provide Diffserv node behavior for the specified application type.

```
-> show lldp port 2/47 remote-system med inventory
Remote LLDP Agents on Local Slot/Port 1/22:
  Remote ID  1:
    MED Hardware Revision = "1.2.12.3",
    MED Firmware Revision = "7.3.2.1",
    MED Software Revision = "4.2.1.11",
    MED Serial Number        = "32421",
    MED Manufacturer Name = "Manufacturer1",
    MED Model Name = "Alc32d21",
    MED Asset ID = "124421",
  Remote ID  2:
    MED Hardware Revision = "1.2.12.4",
    MED Firmware Revision = "7.3.2.2",
    MED Software Revision = "4.2.1.13",
    MED Serial Number        = "32424",
    MED Manufacturer Name = "Manufacturer2",
    MED Model Name = "Alc32d41",
    MED Asset ID = "124424",
```

output definitions

Remote ID	The Index of the Remote Device.
MED Hardware Revision	The Hardware Revision of the endpoint
MED Firmware Revision	The Firmware Revision of the endpoint.
MED Software Revision	The Software Revision of the endpoint.
MED Manufacturer Name	The Manufacturer Name of the endpoint.
MED Model Name	The Model Name of the endpoint.
MED Asset ID	The Asset ID of the endpoint.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

show lldp local-port	Displays per port information.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpV2XMedRemMediaPolicyTable
   lldpV2XMedRemMediaPolicyAppType
   lldpV2XMedRemMediaPolicyDscp
   lldpV2XMedRemMediaPolicyPriority
   lldpV2XMedRemMediaPolicyTagged
   lldpV2XMedRemMediaPolicyUnknown
   lldpV2XMedRemMediaPolicyVlanID
lldpV2XMedRemInventoryTable
   lldpV2XMedRemAssetID
   lldpV2XMedRemFirmwareRev
   lldpV2XMedRemHardwareRev
   lldpV2XMedRemMfgName
   lldpV2XMedRemModelName
   lldpV2XMedRemSerialNum
   lldpV2XMedRemSoftwareRev
```

show lldp remote-system application-tlv

Displays remote system Application Priority TLV information for a single port or all ports on a slot.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port *chassis/slot/port2***[-***port***] | slot** *chassis/slot***] remote-system application-tlv**

Syntax Definitions

non-tpmr	The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
nearest-customer	The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
nearest-bridge	The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	The slot number for a specific module.

Defaults

By default, a list of all LLDP ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the *slot/port* or *slot* parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp remote-system application-tlv
Slot/    Remote
 Port      ID        Selector                       Protocol     Priority
------+----------+-------------------------------+-----------+------------+
  1/2           1    Ethertype                       35078         3 [fcoe]
  1/2           1    Tcp/Sctp                        3260          4 [iscsi]
  1/20          1    Tcp/Sctp                        3190          3
  1/20          1    Udp/Dccp                        300           4
  1/20          1    Tcp/Udp/Sctp/Dccp               300           4
```

output definitions

Slot/Port	The Slot number to which the remote system entry is associated and the physical port number on that module.
Remote ID	The Index of the Remote Device.

output definitions (continued)

Selector	The protocol selector.
Protocol	The protocol Ethertype or well-known port.
Priority	The 802.1p priority value for the specified protocol to use.

Release History

Release 7.3.2; command introduced.

Related Commands

lldp tlv application	Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port.
lldp tlv application priority	Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.
show lldp config	Displays the general LLDP configuration information for LLDP ports.

MIB Objects

```
alaXdot1dcbxAdminApplicationPriorityAppTable
   alaXdot1dcbxAdminApplicationPriorityAESelector
   alaXdot1dcbxAdminApplicationPriorityAEProtocol
   alaXdot1dcbxAdminApplicationPriorityAEPriority
```

show lldp agent-destination-address

Displays the destination address of each agent.

show lldp agent-destination-address

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show lldp agent-destination-address
Lldp                                  Destination
Agent      Name                       MAC address
------+----------------------------------+-----------------------
 1       Nearest-Bridge                   00-80-C2-00-00-0E
 2       Non-TPMR-Bridge  Tcp/Sctp        00-80-C2-00-00-03
 3       Nearest-Customer-Bridge          00-80-C2-00-00-00
```

output definitions

Lldp Agent	The LLDP agent identifier.
Name	The name of the LLDP agent.
Destination MAC address	The destination MAC address of the LLDP agent.

Release History

Release 7.3.1; command introduced.

Related Commands

lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, slot, or port.

MIB Objects

```
lldpV2DestAddressTable
   lldpV2AddressTableIndex
   lldpV2DestMacAddress
```

lldp trust-agent

Enables or disables the security mechanism globally (chassis level) or for a slot or a single port. By enabling LLDP security mechanism on a port, LLDP CMM task brings the LLDP status of the port as trusted and monitors the port for any LLDP security violation.

lldp {*chassis/slot/port* | *chassis/slot* | **chassis} trust-agent** [**admin-state] {enable** | **disable}] [chassis-id-subtype {chassis-component** | **interface-alias** | **port-component** | **mac-address** | **network-address** | **interface-name** | **locally-assigned** | **any}]**

Syntax Definitions

chassis/slot/port	The chassis ID, slot, and port number for the module and the physical port number on that module (for example, 1/2/4 specifies chassis 1, port 4 on slot 2).
chassis/slot	The chassis ID and slot number for the module (for example, 1/2 specifies chassis 1, slot 2).
chassis	Specifies all the ports in the chassis.
enable	Enables LLDP security mechanism.
disable	Disables LLDP security mechanism.
chassis-component	The chassis component is used for validating the remote agent.
interface-alias	The alias configured for the interface is used for validating the remote agent.
port-component	The port component is used for validating the remote agent.
mac-address	The MAC address is used for validating the remote agent.
network-address	The network address is used for validating the remote agent.
interface-name	The interface name is used for validating the remote agent.
locally-assigned	The locally assigned component is used for validating the remote agent, that is the chassis information, which can be locally assigned (the local configuration)
any	The remote agent with any chassis ID sub type is accepted as a trust agent.

Defaults

‘**any**’ - If the chassis ID sub type is not configured for validating the remote agent, by default, the first remote agent is accepted as a trust agent considering any of the chassis ID sub types.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- By enabling security on chassis/slot level, the ports that come under the respective level are monitored for any LLDP security violation.
- If the chassis ID sub type is not configured for validating the remote agent, then the LLDP learns the first remote agent with available chassis ID TLV (Time, Length, Value) received in the PDU.
- After a link up is received on a LLDP security enabled port, LLDP CMM waits for three times the LLDP timer interval (30 seconds). If no LLDP PDU is received after link up that has no remote agent, the port is moved to a violation state.
- If a trusted remote agent already exists, and if no LLDP remote agent is learned even after three times the LLDP timer interval (30 seconds), the port is moved to a violation state. If a new LLDP remote agent is learned after the link toggle, then the port is moved to a violation state.
- If the same chassis ID and port ID already exist in the trusted remote agent database but on a different port, then the port remote agent is learned and the port is moved to a violation state. If a new LLDP remote agent is learned on a port that has a trusted LLDP remote agent, then the port is moved to a violation state.

Examples

```
-> lldp chassis trust-agent admin-state enable
-> lldp chassis trust-agent chassis-id-subtype chassis-component
```

Release History

Release 8.3.1; command introduced.

Related Commands

lldp trust-agent violation-action	Sets the action to be performed when a violation is detected.
show lldp trusted remote-agent	Displays information on trusted remote-agents.
show lldp trust-agent	Displays information on local LLDP agent or port.

MIB Objects

```
alaLldpTrustAdminStatus
   alaLldpTrustChassisIdSubType
```

lldp trust-agent violation-action

Sets the action to be performed when a violation is detected.

lldp {*chassis/slot/port* | *chassis/slot* | **chassis} trust-agent violation-action {trap-and-shutdown | trap | shutdown}**

Syntax Definitions

chassis/slot/port	The chassis ID, slot, and port number for the module and the physical port number on that module (for example, 1/2/4 specifies chassis 1, port 4 on slot 2).
chassis/slot	The chassis ID and slot number for the module (for example, 1/2 specifies chassis 1, slot 2).
chassis	All switch ports.
trap-and-shutdown	Shuts down the port and sends a trap notification when a violation is detected.
trap	Sends a trap notification when a violation is detected.
shutdown	Shuts down the port when a violation is detected.

Defaults

By default, trust agent violation action is set to ‘trap’.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the port is in a shutdown state, clear the violation on the port by using the command “**interfaces** *chassis/slot***[***/port***[-***port2***]] clear-violation-all**”
- Clearing the violation on a port does not clear the trusted remote agent existing on that port. To clear the trusted remote agent, disable the LLDP security mechanism on the port.
- If the port is in a shutdown state due to violation and the port link is toggled, only the link goes up. The port still remains in the violation state and the trusted remote agent existing on that port is not cleared.

Examples

```
-> lldp chassis trust-agent violation-action trap
-> lldp slot 3 trust-agent violation-action shutdown
```

Release History

Release 8.3.1; command introduced.

Related Commands

lldp trust-agent	Sets the status of trust admin status for a port.
show lldp trusted remote-agent	Displays information on trusted remote-agents.
show lldp trust-agent	Displays information on local LLDP agent or port.

MIB Objects

```
alaLldpTrustAction
```

show lldp trusted remote-agent

Displays information on trusted remote-agents.

show lldp [*chassis/slot* **|** *chassis/slot/port***] trusted remote-agent**

Syntax Definitions

chassis/slot	The chassis ID and slot number for the module (for example, 1/2 specifies chassis 1, slot 2).
chassis/slot/port	The chassis ID, slot, and port number for the module and the physical port number on that module (for example, 1/2/4 specifies chassis 1, port 4 on slot 2).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the slot/port or slot parameter to display information for a specific port or for all ports on a specific module.
- LLDP trust agent must be enabled globally on the chassis or individually on a port in order to get the **show lldp trusted remote-agent** command output.

Examples

```
-> lldp chassis trust-agent enable
-> lldp chassis trust-agent chassis-id-subtype mac-address

-> show lldp trusted remote-agent

Trusted Remote LLDP Agents on Local Slot/Port: 1/7
  Chassis ID Subtype          = 4 (MAC Address),
  Chassis ID                  = 00:e0:b1:7a:e6:3c,
  Port ID Subtype             = 7 (Locally assigned),
  Port ID                     = 1017
```

output definitions

Trusted Remote LLDP Agents on Local Slot/Port	The slot number to which the remote trusted agent is associated and the physical port number on that module.
Chassis ID Subtype	The sub type that describes the chassis ID.
Chassis ID	The chassis ID (MAC address).
Port ID Subtype	The sub type that describes port ID.
Port ID	The port ID (Port MAC).

Release History

Release 8.3.1; command introduced.

Related Commands

lldp trust-agent	Sets the status of trust admin status for a port.
lldp trust-agent violation-action	Sets the action to be performed when a violation is detected.
show lldp trust-agent	Displays information on local LLDP agent/port.

MIB Objects

N/A

show lldp trust-agent

Displays information of the local LLDP agent or port.

show lldp [*chassis/slot* **|** *chassis/slot/port***] trust-agent**

Syntax Definitions

chassis/slot	The chassis ID and slot number for the module (for example, 1/2 specifies chassis 1, slot 2).
chassis/slot/port	The chassis ID, slot, and port number for the module and the physical port number on that module (for example, 1/2/4 specifies chassis 1, port 4 on slot 2).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *slot/port* or *num* (slot number) values to display information for a specific port or for all ports on a specific module.
- LLDP trust agent must be enabled globally on the chassis or individually on a port in order to get the **show lldp trust-agent** command output correctly.
- If LLDP security is disabled this command correctly displays the ‘Admin Status’ as ‘Disabled’; however the other output parameters will display their default values.

Examples

```
-> lldp chassis trust-agent enable

-> lldp chassis trust-agent chassis-id-subtype chassis-component

-> show lldp trust-agent

Slot/Port  Admin Status   Violation Action  Violation Status   Chassis Subtype
---------+--------------+-----------------+------------------+-----------------
   1/1     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/2     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/3     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/4     Disabled       Shutdown          Violated           1(Chassis Component)
   1/5     Enabled        Shutdown          Trusted            1(Chassis Component)
   1/6     Enabled        Trap-and-Shutdown Trusted            1(Chassis Component)
   1/7     Disabled       Trap-and-Shutdown Violated           1(Chassis Component)
   1/8     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/9     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/10    Enabled        Trap Only         Trusted            1(Chassis Component)
```

output definitions

Slot/Port	The LLDP slot and port number.
Admin Status	Indicates the administrative status of the LLDP port, **Enabled** or **Disabled**
Violation Action	Indicates the action performed when a violation is detected. The options are - **Trap Only**, **Trap-and-Shutdown**, and **Shutdown Only**.
Violation Status	The violation status of the port, **Trusted** or **Violated**
Chassis Subtype	The sub type that describes the chassis ID.

Release History

Release 8.3.1; command introduced.

Related Commands

lldp trust-agent	Sets the status of trust admin status for a port.
lldp trust-agent violation-action	Sets the action to be performed when a violation is detected.
show lldp trusted remote-agent	Displays information on trusted remote-agents.

MIB Objects

N/A

17 SIP Commands

SIP Snooping feature address the key challenge of real time delivery and monitoring requirements for media streams from SIP devices. SIP snooping feature provides plug and play support to the device, where it automatically identifies the ports used. It also enhances the security of device.

SIP Snooping prioritizes voice and video traffic over non-voice traffic. To summarize, SIP Snooping:

- Identifies and marks the SIP and its corresponding media streams. Each media stream contains Real Time Protocol (RTP) and Real Time Control Protocol (RTCP) flows. Marking is done using the DSCP field in the IP header.
- Provides user configured QOS treatment for SIP/RTP/RTCP traffic flows based on its marking.
- Also snoops voice quality metrics of media streams from their RTCP packets and displays them to the user with knowledge of media reception quality in real time and helps to diagnose the problems on their quality. Also in addition, trap will be generated when voice quality parameters like Jitter, Round trip time, Packet-lost, R-factor and MOS values of media streams crosses user configured threshold.

This chapter includes SIP commands and their descriptions..

MIB information for SIP commands is as follows:

Filename: ALCATEL-IND1-SIP-SNOOPING-MIB.mib
Module: aluSIPSnoopingMIB

A summary of the available commands is listed here:

sip-snooping admin-state

Enables or disables the SIP snooping on the switch.

sip-snooping admin-state {enable | disable}

Syntax Definitions

enable	Enables SIP snooping
disable	Disables SIP snooping

Defaults

By default, SIP-snooping is disabled on the switch.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- If SIP snooping is disabled at the port level, enabling SIP snooping globally will not override the configuration of that port.
- If SIP snooping is disabled and enabled, it is mandatory that the phones re-register for successful DSCP marking.

Examples

```
-> sip-snooping admin-state enable
-> sip-snooping admin-state disable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

sip-snooping port admin-state	Configures the status of SIP snooping on a single port, a range of ports, or on a link aggregate of ports.
show sip-snooping ports	Shows the SIP snooping port level data.
show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

`aluSIPSnoopingStatus`

sip-snooping port admin-state

Configures the status of SIP snooping on a single port, a range of ports, or on a link aggregate.

sip-snooping {port *chassis/slot/port***[-***port2***] | linkagg** *agg_num***} admin-state {enable | disable}**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
agg_num	A link aggregate ID number.
enable	Enables SIP snooping to mirror all SIP PDU that ingress on that port
disable	Disables SIP snooping and will not mirror SIP PDU that ingress on that port.

Defaults

By default, SIP snooping is disabled on the switch.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- Use this command for port/linkagg level SIP Snooping configuration on the switch.
- SIP snooping must be enabled globally to activate port/linkagg level configuration.
- Even after SIP snooping is globally disabled, port/linkagg level configuration is saved. This configuration will be used when SIP snooping is enabled globally again.
- Port level configuration is not allowed on a member port of a linkagg.
- If a port joins a linkagg, port level configuration is overridden by the linkagg configuration. Port level configuration will be activated if the port leaves the linkagg.

Examples

```
-> sip-snooping port 1/1/5-6 admin-state enable
-> sip-snooping linkagg 1 admin-state enable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping ports	Shows the SIP snooping port level data.

MIB Objects

```
aluSIPSnoopingSlotPortIndex
   aluSIPSnoopingRowStatus
```

sip-snooping mode

Configures the SIP snooping mode for the specified port or link aggregate.

sip-snooping {port *chassis/slot/port***[-***port2***] | linkagg** *agg_num***} mode {force-edge | force-non-edge | automatic}**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
agg_num	The link aggregate ID number.
force-edge	Media TCAM entries to be created for dialogs that transverse the specific port
force-non-edge	No Media TCAM entries for dialogs that transverse the specific port.
automatic	Sets to default mode. The port's edge/non-edge mode is derived by the switch/router based on LLDP received or not on the port.

Defaults

By default, the SIP snooping mode is set to automatic.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- Use this command for port/linkagg level SIP Snooping configuration on the switch.
- Force-edge-port/force-non-edge port option to overwrite default port mode learned by either received or not received switch/router capability through LLDP.
- Port level configuration is not allowed on a member port of a linkagg.
- If a port joins a linkagg, port level configuration is overridden by linkagg configuration. Port level configuration will be activated if it leaves the linkagg.

Examples

```
-> sip-snooping port 1/1/5-6 mode force-edge
-> sip-snooping linkagg 1 mode force-non-edge
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping ports	Shows the SIP snooping port level data.

MIB Objects

```
aluSIPSnoopingSlotPortIndex
   aluSIPSnoopingPortConfigPortMode
```

sip-snooping trusted server

Configure the IP addresses of the trusted servers on a switch.

sip-snooping trusted-server [*ip_address1 ip_address2 ip_address ...ip_address8***]**

no sip-snooping trusted-server {*ip_address* **| all}**

Syntax Definitions

*ip_address*1**[-***ip_address2***]**	The IP address of one or more trusted servers.
all	Specifies all the IP addresses.

Defaults

By default, no trusted servers are configured. All SIP based calls using any call server will be supported.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- This command is used to configure the IP addresses of the trusted servers. If a trusted server is configured, then only the calls initiated through those servers will be supported.
- A maximum of 8 trusted servers can be configured.
- If no trust servers are configured, all SIP based calls using any call server will be supported.
- Use the **no** form of the command to remove any trusted IP or all trusted IP addresses.

Examples

```
-> sip-snooping trusted-server 192.254.32.22 192.254.32.33
-> no sip-snooping trusted-server 192.254.32.22
-> no sip-snooping trusted-server all
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingSIPTrustedServerIPAddress1
aluSIPSnoopingSIPTrustedServerIPAddress2
aluSIPSnoopingSIPTrustedServerIPAddress3
aluSIPSnoopingSIPTrustedServerIPAddress4
aluSIPSnoopingSIPTrustedServerIPAddress5
aluSIPSnoopingSIPTrustedServerIPAddress6
aluSIPSnoopingSIPTrustedServerIPAddress7
aluSIPSnoopingSIPTrustedServerIPAddress8
```

sip-snooping sip-control

Configures SIP control DSCP marking.

sip-snooping sip-control dscp *num*

sip-snooping sip-control no dscp

Syntax Definitions

num	The DSCP number. The valid range is 1–4 Mbps.

Defaults

By default no marking/prioritizing or rate limit is performed.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- This command is used for the SIP control DSCP marking. A built-in rate limiter of 1 Mbps is configured to rate limit SIP PDUs being marked by the switch.
- The packet gets its priority as normal packet, either from the QoS port configuration (trust the packet DSCP or untrusted) or from a user configured QoS policy.
- Use **no** form of the command is to set default mode.

Examples

```
-> sip-snooping sip-control dscp 40
-> sip-snooping sip-control no dscp
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

`aluSIPSnoopingSIPControlDSCP`

sip-snooping sos-call number

Configures the SOS call strings in SIP snooping.

sip-snooping sos-call number *string1 string2* **…** *string4*

no sip-snooping sos-call number {*string* | **all}**

Syntax Definitions

string1 **…** *string4*	Specifies the SOS call string.
all	Specifies all the SOS call strings.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- This command is used for the configuration of the SOS call strings. A maximum of 4 SOS call strings can be configured for an exact match on the “to” URI (user part only)
- No support of regular expression. If no string is specified, no SOS call can be identified in the system.
- Use **no** form of this command to remove existing SOS call strings.

Examples

```
-> sip-snooping sos-call number “911” “2233”
-> no sip-snooping sos-call number “911”
-> no sip-snooping sos-call number all
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Displays the SIP snooping configuration.

MIB Objects

```
aluSIPSnoopingSOSCallNumber1
aluSIPSnoopingSOSCallNumber2
aluSIPSnoopingSOSCallNumber3
aluSIPSnoopingSOSCallNumber4
```

sip-snooping sos-call dscp

Configures the SOS-Call RTP/RTCP DSCP marking.

sip-snooping sos-call dscp *num*

Syntax Definitions

num	Specifies the DSCP number.

Defaults

The default configuration is 46 EF.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- This command is used for the configuration of the SOS-Call RTP/RTCP DSCP marking. A built-in rate limiter of 128 kbps is configured to rate limit a uni-direction media stream being marked by the switch.
- SOS calls are identified only for the Audio media type. All other media type calls are considered normal calls.

Examples

```
-> sip-snooping sos-call dscp 56
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Displays the SIP snooping configuration for the switch.

MIB Objects

`aluSIPSnoopingSOSCallRTPDSCP`

sip-snooping udp port

Configures the UDP port for SIP Snooping.

sip-snooping udp-port *udp-port1 udp-port 2* **...** *udp-port 8*

no sip-snooping udp-port {*udp-port* **| all}**

Syntax Definitions

udp-port 1 **...** *udp-port 8*	Specifies the UDP port for SIP snooping.
all	Specifies all the UDP ports designated for SIP snooping.

Defaults

By default no UDP ports and SIP mirroring is performed with the method name and SIP2.0 strings.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- A maximum of 8 UDP ports can be configured on a switch.
- Use **no** form of this command to remove any UDP port configured earlier.

Examples

```
-> sip-snooping udp-port 5260 5060
-> no sip-snooping udp-port 5260
-> no sip-snooping udp-port all
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingSIPUDPPort1
aluSIPSnoopingSIPUDPPort2
aluSIPSnoopingSIPUDPPort3
aluSIPSnoopingSIPUDPPort4
aluSIPSnoopingSIPUDPPort5
aluSIPSnoopingSIPUDPPort6
aluSIPSnoopingSIPUDPPort7
aluSIPSnoopingSIPUDPPort8
```

sip-snooping tcp port

Configures the Server listening TCP ports for SIP Snooping.

sip-snooping tcp-port *tcp-port1 tcp-port 2* **...** *tcp-port 8*

no sip-snooping tcp-port {*tcp-port* **| all}**

Syntax Definitions

tcp-port 1 **...** *tcp-port 8*	Specifies the TCP port for SIP snooping.
all	Specifies all the SOS call strings.

Defaults

By default, TCP port is 5260.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- A maximum of 8 TCP ports can be configured on a switch.
- The default port will be overwritten if the user configures any other port.
- Use the **no** form of this command to remove any TCP port configured earlier.

Examples

```
-> sip-snooping tcp-port 5260 5060
-> no sip-snooping tcp-port 5260
-> no sip-snooping tcp-port all
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingSIPTCPPort1
aluSIPSnoopingSIPTCPPort2
aluSIPSnoopingSIPTCPPort3
aluSIPSnoopingSIPTCPPort4
aluSIPSnoopingSIPTCPPort5
aluSIPSnoopingSIPTCPPort6
aluSIPSnoopingSIPTCPPort7
aluSIPSnoopingSIPUDPPort8
```

sip-snooping threshold

Configure the various thresholds of SIP snooping.

sip-snooping threshold {audio | video | other} {jitter *jitter_ms_num* **| packet-lost** *% num* **| round-trip-delay** *round_trip_delay_ms_num* **| r-factor** *rfactor_num*| **mos** *mos_num***}**

Syntax Definitions

audio	Specify threshold for audio.
video	Specify threshold for video.
other	Specify threshold for other.
jitter_ms_num	Specify jitter in milliseconds. The valid range is 0–300.
% num	Specify packet lost in percentage. The valid range is 0–99%.
round_trip_delay_ms_num	Set round trip delay in milliseconds. The valid range is 0–500.
rfactor_num	Specify R-factor number. The valid range is 0–100.
mos_num	Specify MOS number. The valid range is 0–5.

Defaults

parameter	default
RTCP monitoring	Enable
Jitter Threshold (audio/video/other)	50/100/100 ms
Packet-lost Threshold (audio/video/other)	10 /20/20%
RTT Threshold (audio/video/other)	180 /250/250 ms
R-factor Threshold (audio/video/other)	70/80/80
MOS Threshold (audio/video/other)	3.6/3.0/3.0

Platforms Supported

OmniSwitch 6860

Usage Guidelines

Setting a threshold value to 0 disables threshold checking for that parameter.

Examples

```
-> sip-snooping threshold audio jitter 50
-> sip-snooping threshold audio packet-lost 10
-> sip-snooping threshold video jitter 80
-> sip-snooping threshold video round-trip-delay 180
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Shows the configuration done for SIP snooping.

MIB Objects

```
aluSIPSnoopingThresholdMediumIndex
   aluSIPSnoopingThresholdMedium
   aluSIPSnoopingThresholdJitter
   aluSIPSnoopingThresholdPacketLost
   aluSIPSnoopingThresholdRoundTripDelay
   aluSIPSnoopingThresholdRFactor
   aluSIPSnoopingThresholdMOS
```

sip-snooping logging-threshold num-of-calls

Configures the threshold for the number of calls to be logged into the flash file.

sip-snooping logging-threshold num-of-calls *num*

Syntax Definitions

num	Specifies the maximum number of calls to be logged.

Defaults

By default, 200 calls can be logged.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This command is used to configure the threshold for the number of calls to be logged into the flash file.

Examples

```
-> sip-snooping logging-threshold num-of-calls 300
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Displays the SIP snooping configuration for the switch.

MIB Objects

```
aluSIPSnoopingThresholdNumberOfCalls
```

show sip-snooping call-records

Displays the SIP-snooping active/ended call records.

show sip-snooping call-records {active-calls | ended-calls} [full | threshold-violation]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This command is used to show the SIP-snooping active/ended call records.

Examples

```
-> show sip-snooping call-records ended-calls full
Legend: start date time duration media-type end-reason
         call-id / from-tag / to-tag
         IP address port DSCP (forward/reverse)
         policy-rule (F/R)
         Pkt count (F/R)
         statistics min / max / avg %samples exceeding threshold (F/R)

------------------------------------------------------------------------
2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
01234567890123456789012345678901234567890123456789012345678901234567890123 /
01234567890123456789012345678901 / 01234567890123456789012345678901
IP/DSCP 222.222.222.222 22222 63/63 111.111.111.111 11111 63/63
Policy-Rule SIP-VLAN10-Rule              SIP-VLAN10-Rule
Pkt-Count 9999999999                     9999999999
Pkt-Loss   99.9 /  99.9 /  99.9 99%       99.9 /  99.9 /  99.9 99%
Jitter    999.9 / 999.9 / 999.9 99%      999.9 / 999.9 / 999.9 99%
Delay     99999 / 99999 / 99999 99%      99999 / 99999 / 99999 99%
R-factor   99.9 / 99.9  / 99.9            99.9 / 99.9  / 99.9
MOS         4.9 / 4.9   / 4.9              4.9 / 4.9   / 4.9


2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
1j9FpLxk3uxtm8tn@biloxi.example.com / a73kszlf / 1410948204
IP/DSCP   135.254.170.110 18888 46/32    125.54.110.110 29996 46/32
Policy-Rule SIP-Audio-SRCIP              SIP-AUDIO-VLAN100
Pkt-Count 10000                          12000
Pkt-Loss   0.9  /     0 / 2.8  0%         0   / 0      / 1   0%
Jitter      3.7 /     0 / 9    0%       0.1   / 0      / 0.2 0%
Delay      50.1 / 44    / 108
R-factor   70.1 / 55    / 77   0%        70.1 / 55    / 77   0%
```

```
MOS         4.1 / 3.9   / 4.2  0.1%       4.1 / 3.9   / 4.2  0.1%

------------------------
Number of Call Records: 2

-> show sip-snooping call-records ended-calls
Legend: start date time duration media-type end-reason
         call-id / from-tag / to-tag
         IP address port DSCP (forward/reverse)
         policy-rule (F/R)

------------------------------------------------------------------------
2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
01234567890123456789012345678901234567890123456789012345678901234567890123 /
01234567890123456789012345678901 / 01234567890123456789012345678901
IP/DSCP 222.222.222.222 22222 63/63 111.111.111.111 11111 63/63
Policy-Rule SIP-VLAN10-Rule              SIP-VLAN10-Rule

2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
1j9FpLxk3uxtm8tn@biloxi.example.com / a73kszlf / 1410948204
IP/DSCP   135.254.170.110 18888 46/32    125.54.110.110 29996 46/32
Policy-Rule SIP-Audio-SRCIP              SIP-AUDIO-VLAN100

------------------------
Number of Call Records: 2

-> show sip-snooping call-records active-calls threshold-violation
Legend: start date time duration media-type end-reason
         call-id / from-tag / to-tag
         IP address port DSCP (forward/reverse)
         policy-rule (F/R)
         statistics min / max / avg %samples exceeding threshold (F/R)

------------------------------------------------------------------------
2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio -
1j9FpLxk3uxtm8tn@biloxi.example.com / a73kszlf / 1410948204
IP/DSCP   135.254.170.110 18888 46/32    125.54.110.110 29996 46/32
Policy-Rule SIP-AUDIO-SRCIP              SIP-AUDIO-VLAN100
MOS         4.1 / 3.9   / 4.2  0.1%       4.1 / 3.9   / 4.2  0.1%
------------------------
Number of Call Records: 1
```

output definitions

Policy-Rule	Name of the SIP policy rule.
Pkt-Count	Packet Count in percentage for SIP Snooping.
Pkt-Loss	Packet Loss in percentage for SIP Snooping.
Jitter	Jitter threshold in millisec for SIP Snooping.
Delay	Round trip delay in millisec for SIP Snooping.
R-factor	R-Factor for SIP Snooping.
MOS	MOS for SIP Snooping.
Number of Call Records	Number of call records that can be stored onto the device.

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config	Displays the SIP snooping configuration.

MIB Objects

```
alaQoSDSCPEntryNumber
alaQoSDSCPPriority
alaQoSDSCPDropPrecedence
```

clear sip-snooping statistics

Clears all the values of SIP snooping statistics

clear sip-snooping statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This command is used to clear all the SIP-snooping statistics.

Examples

```
-> clear sip-snooping statistics
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping statistics	Displays SIP snooping statistics.

MIB Objects

```
aluSIPSnoopingClearStats
```

show sip-snooping config

Displays the SIP snooping configuration for the switch.

show sip-snooping config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This command is used to show the SIP snooping status and configuration for the switch.

Examples

```
-> show sip-snooping config
Sip-snooping Status : Enable,
Sip-control DSCP : 40,
SOS-Call RTP/RTCP DSCP : 35,
SOS-Call Number : 911, 2233,
Jitter Threshold (audio/video/other) : 50ms/100ms/100ms,
Packet-Lost Threshold (audio/video/other) : 10/20/20,
Round-Trip-Delay Threshold (audio/video/other) : 180ms/250ms/250ms,
R-factor Threshold (audio/video/other) : 70/80/80,
MOS Threshold (audio/video/other) :3.6/3.0/3.0 ,
Logging Number of calls : 200,
UDP-Port(s) : 5060, 5260
TCP-Port(s) : 5260
Trusted Server IP(s) : 192.254.32.11,192.254.32.22,192.254.32.33
Reserved HW resource : 1,
CPU Rate Limiter for SIP PDUS : 1 mbps,
```

output definitions

Sip-snooping Status	Indicates whether the SIP Snooping status is Enable or Disable.
Sip-control DSCP	Displays the SIP control DSCP value
SOS-Call RTP/RTCP DSCP	Displays the SOS-Call RTP/RTCP DSCP number.
SOS-Call Number	Displays the emergency call number.
Jitter Threshold	Displays the Jitter threshold in milliseconds.
Packet-Lost Threshold	Displays the packet lost threshold in percentage.
Round-Trip-Delay Threshold	Displays the Round-Trip-Delay threshold period in milliseconds.
R-factor Threshold	Displays the R-Factor value.

output definitions (continued)

MOS Threshold	Displays the MOS for SIP Snooping.
Logging Number of calls	Displays the maximum number of calls to be logged in flash file
UDP-Ports	Displays the SIP Snooping UDP Ports.
TCP Ports	Displays the SIP Snooping TCP ports.
Trusted Server IP(s)	Displays the truster server IP addresses.

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping statistics	Displays SIP snooping statistics.
clear sip-snooping statistics	Clears all the logs of SIP snooping statistics

MIB Objects

```
aluSIPSnoopingThresholdMediumIndex
   aluSIPSnoopingStatus
   aluSIPSnoopingSIPControlDSCP
   aluSIPSnoopingSOSCallRTPDSCP
   aluSIPSnoopingSOSCallNumber1
   aluSIPSnoopingSOSCallNumber2
   aluSIPSnoopingSOSCallNumber3
   aluSIPSnoopingSOSCallNumber4
   aluSIPSnoopingThresholdMedium
   aluSIPSnoopingThresholdJitter
   aluSIPSnoopingThresholdPacketLost
   aluSIPSnoopingThresholdRoundTripDelay
   aluSIPSnoopingThresholdNumberOfCalls
   aluSIPSnoopingSIPTrustedServerIPAddress1
   aluSIPSnoopingSIPTrustedServerIPAddress2
   aluSIPSnoopingSIPTrustedServerIPAddress3
   aluSIPSnoopingSIPTrustedServerIPAddress4
   aluSIPSnoopingSIPTrustedServerIPAddress5
   aluSIPSnoopingSIPTrustedServerIPAddress6
   aluSIPSnoopingSIPTrustedServerIPAddress7
   aluSIPSnoopingSIPTrustedServerIPAddress8
   aluSIPSnoopingSIPUDPPort1
   aluSIPSnoopingSIPUDPPort2
   aluSIPSnoopingSIPUDPPort3
   aluSIPSnoopingSIPUDPPort4
   aluSIPSnoopingSIPUDPPort5
   aluSIPSnoopingSIPUDPPort6
   aluSIPSnoopingSIPUDPPort7
   aluSIPSnoopingSIPUDPPort8
```

show sip-snooping ports

Displays configuration information for SIP snooping ports.

show sip-snooping ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This command is used to show the SIP-snooping port-level data.

Examples

```
-> show sip-snooping ports
Legend : sip snooping : * status disabled (Sip-snooping globally disabled)
Port       sip-snooping         Edge/Non-edge
-----------------------------------------------------
1/1        enable               automatic
1/3        enable (*)           force-edge
1/3        enable (*)           force-non-edge
```

output definitions

Port	Displays ports configured for sip-snooping.
sip-snooping	Displays the status of sip-snooping on the port, **enable** or **disable**.
Edge/Non-edge	Displays the edge status of the port.

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping statistics	Displays SIP snooping statistics.

MIB Objects

```
aluSIPSnoopingPortConfigSlotPortIndex
   aluSIPSnoopingPortConfigPortStatus
   aluSIPSnoopingPortConfigPortMode
```

show sip-snooping statistics

Displays SIP snooping statistics.

show sip-snooping statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This command is used to show the SIP snooping statistics.

Examples

```
-> show sip-snooping statistics
Total calls processed                  : ,
Total audio streams                    : ,
Total video streams                    : ,
Total other streams                    : ,
Total audio streams that crossed threshold       : ,
Total video streams that crossed threshold       : ,
Total other streams that crossed threshold       : ,
Active Streams that crossed threshold            : ,
Number of Active calls                 : ,
Number of active audio streams         : ,
Number of active video streams         : ,
Number of active other streams         : ,
Number of SIP packet received by hardware :
Number of SIP packet received by software :
Number of SIP packet received per method: INVITE(100) ACK(101) BYE(200)
UPDATE(40) PRACK(20)
Number of SIP response packet received:
Number of discarded/malformed/unsupported SIP packets:
Number of discarded SIP packets not from/to trusted servers:
Number of dropped SIP packet due the software error:
(NI overflow, NI/CMM, CMM overflow)
Total Emergency Calls                  :
```

output definitions

Total calls processed	Total calls processed for SIP Snooping.
Total audio streams	Displays the total audio streams.
Total video streams	Displays the total video streams.

output definitions (continued)

Total other streams	Displays the total other streams.
Total audio streams that crossed threshold	Displays the total audio streams that have exceeded threshold.
Total video streams that crossed threshold	Displays the total video streams that have exceeded threshold.
Total other streams that crossed threshold	Displays the total other streams that have exceeded threshold.
Number of Active calls	Displays the number of active calls.
Number of Active audio streams	Displays the number of active audio streams.
Number of Active video streams	Displays the number of active video streams.
Number of Active other streams	Displays the number of active other streams.
Number of SIP packet received by hardware	Displays the total SIP packet received by hardware.
Number of SIP packet received by software	Displays the total SIP packet received by software.
Number of SIP packet received by per method	Displays the method by which the SIP packet is received. The various per method are Invite, Ack, Bye, Update and Prack.
Number of SIP response packet received	Displays the total number of SIP response packet received.
Number of discarded/ malformed/unsupported SIP packets	Displays the total number of discarded, malformed or unsupported SIP packets.
Number of discarded SIP packets not from/to trusted servers	Displays the total number of discarded SIP packets not from or to trusted servers
Number of dropped SIP packet due the software error	Displays the Total number of SIP packets dropped due the software error. (i.e. NI overflow, NI/CMM, CMM overflow etc.)
Total Emergency Calls	Displays the total number of Emergency Calls.

Release History

Release 8.1.1; command was introduced.

Related Commands

clear sip-snooping statistics	Clears the SIP snooping statistics.

MIB Objects

```
aluSIPSnoopingTotalCallsProcessed
aluSIPSnoopingTotalAudioStreams
aluSIPSnoopingTotalVideoStreams
aluSIPSnoopingTotalOtherStreams
aluSIPSnoopingAudioStreamsBeyondThreshold
aluSIPSnoopingVideoStreamsBeyondThreshold
aluSIPSnoopingOtherStreamsBeyondThreshold
aluSIPSnoopingActiveStreamsBeyondThreshold
aluSIPSnoopingActiveAudioStreams
aluSIPSnoopingActiveVideoStreams
aluSIPSnoopingActiveOtherStreams
aluSIPSnoopingHardwareSIPPackets
aluSIPSnoopingSoftwareSIPPackets
aluSIPSnoopingSIPInvitePackets
aluSIPSnoopingSIPAckPackets
aluSIPSnoopingSIPByePackets
aluSIPSnoopingSIPByePackets
aluSIPSnoopingSIPUpdatePackets
aluSIPSnoopingSIPPrackPackets
aluSIPSnoopingSIPRecvdResponsePackets
aluSIPSnoopingSIPDiscardedPackets
aluSIPSnoopingSIPDiscardedNoTrustServerPackets
aluSIPSnoopingSIPDroppedSWErrorPackets
aluSIPSnoopingTotalEmergencyCalls
```

show sip-snooping registered-clients

Shows the registered SIP clients learned by the switch.

show sip-snooping registered-clients

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This command is used to show the registered SIP clients learned by the switch.

Examples

```
-> show sip-snooping registered-clients

 S/N           Registered Client IP Address
-----------------------------------------------
 1               10.135.22.18
 2               10.135.22.25
 3               10.135.23.124
```

output definitions

Registered Client IP Address	The IP address of the registered client.

Release History

Release 8.1.1; command was introduced.

Related Commands

sip-snooping port admin-state	Configures the status of SIP snooping on a single port, a range of ports, or on a link aggregate.

MIB Objects

```
alaSIPSnoopingRegisteredClientNumber
alaSIPSnoopingRegisteredClientAddrType
alaSIPSnoopingRegisteredClientAddr
```

18 Automatic Fabric Commands

The Dynamic Auto-Fabric feature can be used to bring up AOS compatible devices by automating some tedious and complex steps including Link Aggregate formation, and SPB neighbor adjacency formation. Dynamic recognition of the neighboring elements will allow a quick, out-of-the box configuration. The focus area for this feature is data center but the feature is applicable in campus LAN environment to reduce administrative overhead.

Upon boot-up the system will automatically attempt auto discovery of LACP, SPB, MVRP, and IP connections if configuration files are not available in the device. The feature allows to build a true fabric when a device is plugged to the network and automates edge port configuration with profiles.

MIB information for the Auto Fabric commands is as follows:

Filename: ALCATEL-IND1-AUTO-FABRIC-MIB.mib
Module: alcatelIND1AUTOFABRICMIB

A summary of available commands is listed here:

auto-fabric admin-state

Enables or disables the Automatic Fabric functionality globally for the switch.

auto-fabric admin-state {enable | disable {remove-global-config | remove-vc-reload]}

Syntax Definitions

enable	Enables Automatic Fabric functionality for the switch.
disable	Disables Automatic Fabric functionality for the switch. When disabled, the global configuration settings discovered for MVRP, SPB, and IP are removed
remove-global-config	Disables Automatic Fabric functionality for the switch. This parameter option performs the same function as the **disable** parameter.
remove-vc-reload	Reboots a switch running in the Virtual Chassis (VC) of one mode to run in the standalone mode with Automatic Fabric discovery disabled. *This parameter option is not supported on the OmniSwitch 6860 and OmniSwitch 6865.*

Defaults

By default, the Automatic Fabric operation is globally enabled for the switch and on all eligible interfaces when the switch boots up without a configuration file (such as boot.cfg) or the configuration file size is zero bytes.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- When a switch boots up with an existing configuration file, the Automatic Fabric operation is based on the administrative status setting specified with this command.
- When Automatic Fabric is globally disabled for the switch, the following configuration settings are removed unless they were previously saved to the switch configuration file:
  - Spanning Tree is set back to the default 1x1 mode. This only occurs if there are no VLAN registrations on any port or link aggregate.
  - SPB is globally disabled, which removes BVLANs 4000-4015 and administratively disables SPB. This only occurs if there are no SPB adjacencies formed on any ports or link aggregates.
  - Automatic Fabric strops trying to learn IP routing protocols and neighbors on interfaces not already configured with a routing protocol. The configuration for IP interfaces on which routing protocols were previously discovered is not removed.
  - For any other scenario, administrator intervention is needed to remove the configuration.
- The **remove-global-config** and **remove-vc-config** parameters are only used in combination with the **disable** option.
- The **remove-vc-config** parameter is only meant for use when a switch has booted up in a VC of one mode. Do not use this option if the switch boots up as part of a VC configuration, where the switch is connected to other switches in the VC.

- When this command is used with the **remove-vc-config** parameter, the following process is triggered:

  1 Any Automatic Fabric configuration is cleared.

  2 The Automatic Fabric feature is disabled.

  3 A **boot.cfg** file is created in the /flash/working directory.

  4 The switch is automatically rebooted in standalone mode with a configuration file and the automatic management features will no longer run.

Examples

```
-> auto-fabric admin-state enable
-> auto-fabric admin-state disable
-> auto-fabric admin-state disable remove-global-config
-> auto-fabric admin-state disable remove-vc-reload
```

Release History

Release 7.3.2; command introduced.
Release 7.3.4; **remove-global-config** and **remove-vc-reload** parameters added-

Related Commands

auto-fabric interface	Enables or disables Automatic Fabric discovery on one or more ports.
show auto-fabric config interface	Displays the Automatic Fabric configuration applied to switch ports.

MIB Objects

```
alaAutoFabricGlobalStatus
alaAutoFabricRemoveGlobalConfig
alaAutoFabricRemoveVCReload
```

auto-fabric interface

Enables or disables the Automatic Fabric functionality for one or more switch ports.

auto-fabric interface *chassis/slot/port***[-***port2***] admin-state {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
enable	Enables Automatic Fabric functionality globally or on an interface.
disable	Disables Automatic Fabric functionality on the specified interface. When disabled, the configuration settings discovered for MVRP, SPB, and IP are removed from the port.

Defaults

By default, the Automatic Fabric operation is globally enabled for the switch and on all eligible interfaces when the switch boots up without a configuration file (such as boot.cfg) or the configuration file size is zero bytes.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- When a switch boots up with an existing configuration file, the Automatic Fabric status for a port is based on the administrative status setting specified with this command.
- The Automatic Fabric status for a specific port takes precedence over the global Automatic Fabric status for the switch. For example, if Automatic Fabric is enabled for the switch but disabled on a port, then the discovery process is not run on the port.

Examples

```
-> auto-fabric interface 1/1/1 admin-state disable
-> auto-fabric interface 1/1/5-10 admin-state enable
```

Release History

Release 7.3.2; command introduced.

Related Commands

auto-fabric admin-state	Globally enables or disables Automatic Fabric for the switch.
show auto-fabric config interface	Displays the Automatic Fabric configuration applied to switch ports.

MIB Objects

```
alaAutoFabricPortConfigTable
   alaAutoFabricPortConfigStatus
```

auto-fabric discovery start

Manually starts the Automatic Fabric discovery process.

auto-fabric discovery start

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

This command can be used to manually begin the Automatic Fabric discovery process after the switch has booted and the discovery window has elapsed.

Examples

```
-> auto-fabric discovery start
```

Release History

Release 7.3.2; command introduced.

Related Commands

show auto-fabric config	Displays the global Automatic Fabric configuration.
show auto-fabric config interface	Displays Automatic Fabric configuration applied on interfaces.

MIB Objects

```
alaAutoFabricGlobalDiscovery
```

auto-fabric protocols

Enables or disables the Automatic Fabric discovery process for a particular protocol.

auto-fabric protocols {lacp | mvrp | spb | ip {ospfv2 | ospfv3 | isis | all} | loopback-detection} {interface *chassis/slot/port-port2* **| chassis} admin-state {enable | disable}**

Syntax Definitions

lacp	Selects the Link Aggregation Control Protocol.
mvrp	Selects the Multiple VLAN Registration Protocol.
spb	Selects the Shortest Path Bridging protocol. *This parameter option is not supported on the OmniSwitch 6465 or OmniSwitch 6560.*
ospfv2	Selects the Open Shortest Path First version 2 protocol. *This parameter option is not supported on the OmniSwitch 6465 or OmniSwitch 6560.*
ospfv3	Selects the Open Shortest Path First version 3 protocol. *This parameter option is not supported on the OmniSwitch 6465 or OmniSwitch 6560.*
isis	Selects the Intermediate System-Intermediate System protocol. *This parameter option is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 9900.*
all	Selects all the supported IP routing protocols (OSPFv2, OSPFv3, and IS-IS).
loopback-detection	Selects Loopback Detection for UNP SPB access ports. Access ports are used to create SPB Service Access Points (SAP).
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
chassis	All Automatic Fabric ports on the chassis. Use this parameter to globally configure the discovery status for the selected protocol.
enable	Enables the discovery status for the selected protocol.
disable	Disables the discovery status for the selected protocol.

Defaults

- Automatic Fabric discovery is globally enabled for all the protocols when the switch boots up without a configuration file.
- Automatic Fabric discovery is globally enabled for all protocols, except MVRP, when the switch boots up with an existing configuration file. In this case, the global default setting for MVRP is disabled.
- Automatic Fabric discovery is enabled for LACP, MVRP, and SPB on all eligible interfaces by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- If no interface is specified with this command, the discovery status for the protocol is enabled or disabled globally for the switch.
- The **interface** and **chassis** parameters are only used in combination with the **lacp**, **mvrp**, and **spb** parameters.
- The interface setting for LACP, MVRP, and SPB discovery overrides the global setting. For example, if SPB discovery is globally enabled for the switch but disabled on port 2/1/1, then the port does not participate in the SPB discovery process.

Examples

```
-> auto-fabric protocols lacp admin-state disable
-> auto-fabric protocols mvrp admin-state enable
-> auto-fabric protocols spb interface 1/1/3 admin-state disable
-> auto-fabric protocols loopback-detection admin-state disable
-> auto-fabric protocols ip ospfv2 admin-state enable
-> auto-fabric protocols ip ospfv3 admin-state disable
-> auto-fabric protocols ip isis admin-state disable
```

Release History

Release 7.3.2; command introduced.
Release 7.3.4; **loopback-detection** and **ip** parameters added.
Release 8.3.1; default setting for global MVRP discovery is disabled when switch boots up with an existing configuration file.

Related Commands

auto-fabric admin-state	Enables or disables Automatic Fabric functionality.
auto-fabric discovery start	Manually starts the Automatic Fabric discovery process.
show auto-fabric config interface	Displays the Automatic Fabric configuration applied on interfaces.
show auto-fabric config	Displays the global Automatic Fabric configuration.

MIB Objects

```
   alaAutoFabricGlobalLACPProtocolStatus
   alaAutoFabricGlobalSPBProtocolStatus
   alaAutoFabricGlobalMVRPProtocolStatus
   alaAutoFabricGlobalOSPFv2Status
   alaAutoFabricGlobalOSPFv3Status
   alaAutoFabricGlobalISISStatus
   alaAutoFabricLBDProtocolStatus
alaAutoFabricPortConfigTable
   alaAutoFabricPortLACPProtocolStatus
   alaAutoFabricPortSPBProtocolStatus
   alaAutoFabricPortMVRPProtocolStatus
```

auto-fabric config-save interval

Configures the time interval for saving the automatically discovered configuration to the switch configuration file.

auto-fabric config-save interval *seconds*

Syntax Definitions

seconds	The amount of time between automatic saves of the discovered configuration. Range is 60 - 3600 seconds.

Defaults

parameter	default
seconds	300

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

The automatic save time interval specified with this command is only valid when the automatic configuration save status is enabled. This is done through the **auto-fabric config-save admin-state** command.

Examples

```
-> auto-fabric config-save interval 600
```

Release History

Release 7.3.2; command introduced.

Related Commands

auto-fabric config-save admin-state	Enables or disables automatically saving of the discovered configuration to the switch configuration file
show auto-fabric config	Displays the Automatic Fabric configuration.

MIB Objects

```
alaAutoFabricGlobalConfigSaveTimer
```

auto-fabric config-save admin-state

Enables or disables automatically saving of the discovered configuration to the switch configuration file.

auto-fabric config-save admin-state {enable | disable}

Syntax Definitions

enable	Enables automatically saving the discovered configuration to the switch configuration file.
disable	Disables automatically saving the discovered configuration to the switch configuration file.

Defaults

By default, automatically saving the discovered configuration is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

When this function is enabled, the amount of time specified through the **auto-fabric config-save interval** command is active. An automatic save is performed whenever the specified amount of time elapses.

Examples

```
-> auto-fabric config-save admin-state disable
```

Release History

Release 7.3.2; command introduced.

Related Commands

auto-fabric config-save interval	Configures the amount of time to wait between automatic saves of the discovered configuration.
show auto-fabric config	Displays the Automatic Fabric configuration.

MIB Objects

```
alaAutoFabricGlobalConfigSaveTimerStatus
```

auto-fabric discovery-interval

Configures when the switch will automatically start the Automatic Fabric discovery process.

auto-fabric discovery-interval *minutes*

Syntax Definitions

minutes	The discovery interval time. The valid range is 2–3600 minutes.

Defaults

By default, the discovery interval timer is set to zero (disabled).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- When a switch boots up without a configuration file, discovery is automatically started for a one time, initial run even when the interval timer is disabled.
- Set the value of this timer to more than two times the value of the switch MAC address aging time. This will allow time for inactive MAC addresses to age out on Automatic Fabric ports before the next discovery interval is started.

Examples

```
-> auto-fabric discovery-interval 60
```

Release History

Release 7.3.2; command introduced.
Release 7.3.4; timer default value changed to zero (disabled).

Related Commands

show auto-fabric config	Displays the Automatic Fabric configuration.

MIB Objects

```
alaAutoFabricGlobalDiscoveryTimer
```

auto-fabric protocols spb default-profile

Configures the default Service Access Point (SAP) profile that the Universal Network Profile (UNP) feature uses to dynamically create SAPs for traffic received on UNP SPB access ports.

auto-fabric protocols spb default-profile {single-service | auto-vlan}

Syntax Definitions

single-service	Dynamically creates a SAP profile only for untagged traffic on the UNP SPB access port.
auto-vlan	Dynamically creates a SAP for each VLAN tag received on a UNP SPB access port. When this option is selected, the **single-service** option is automatically triggered for untagged traffic.

Defaults

By default, the switch is set to use the **auto-vlan** option.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- A SAP is a logical service entity (also referred to as a virtual port) that binds an access port to an SPB service ID and specifies the type of customer traffic (untagged or tagged) to encapsulate and tunnel through the SPB network infrastructure.
- Once the SPB adjacencies and UNP access ports are configured through Automatic Fabric discovery, traffic received on UNP access ports triggers the switch to dynamically create a SAP for the traffic based on the SAP profile selected with this command.

Examples

```
-> auto-fabric protocols spb default-profile single-service
-> auto-fabric protocols spb default-profile auto-vlan
```

Release History

Release 7.3.4; command introduced.

Related Commands

auto-fabric protocols spb set-profile	Configures the default SAP profile for a specific port or range of ports on the switch.
show auto-fabric config	Displays the global Automatic Fabric configuration.
show auto-fabric config interface	Displays Automatic Fabric configuration applied on interfaces.

MIB Objects

```
alaAutoFabricSPBDefaultProfile
```

auto-fabric protocols spb set-profile

Configures the default SAP profile for a specific port or range of ports on the switch.

auto-fabric protocols spb set-profile {single-service | auto-vlan} interface *chassis/slot/port***[-***port2***]**

Syntax Definitions

single-service	Defines single default service SAP profile. Only untagged traffic on the UNP-SPB port is learnt in this profile.
auto-vlan	The incoming traffic is automatically learnt. The SAP bindings for the concerned VLANs are automatically created based on the traffic sensed.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1) on which the SAP profile will be enabled. Use a hyphen to specify a range of ports (3/1-8).

Defaults

By default, the **auto-vlan** option is used for Automatic Fabric ports.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

The SAP profile configured for the specified port or range of ports overrides the default SAP profile configured for the switch.

Examples

```
-> auto-fabric protocols spb set-profile single-service interface 1/1/1
-> auto-fabric protocols spb set-profile auto-vlan interface 1/2/1-4
```

Release History

Release 7.3.4; command introduced.

Related Commands

show auto-fabric config	Displays the auto-fabric configuration.
show auto-fabric config interface	Displays auto-fabric configuration applied on interfaces.

MIB Objects

```
alaAutoFabricPortConfigTable
   alaAutoFabricPortConfigIfIndex
   alaAutoFabricPortSPBDefaultProfile
```

show auto-fabric config

Displays the Automatic Fabric configuration.

show auto-fabric config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show auto-fabric config
Auto-fabric Status          : Disable,
Config Save Timer Status    : Disabled,
Config Save Timer Interval  : 300 seconds,
Default UNP SAP Profile     : Auto-vlan,
Discovery Interval          : 1 minute(s),
Discovery Status            : Idle,
LACP Discovery Status       : Enabled,
LBD Discovery Status        : Enabled,
MVRP Discovery Status       : Disabled,
OSPFv2 Discovery Status     : Enabled,
OSPFv3 Discovery Status     : Enabled,
ISIS Discovery Status       : Enabled,
SPB Discovery Status        : Enabled
```

output definitions

Auto-Fabric Status	The global status of the Automatic Fabric functionality.
Config Save Timer Status	Displays the status of the Automatic Fabric configuration save timer.
Config Save Timer Interval	Displays how often the discovered Automatic Fabric configuration is saved to the switch configuration file.
Default UNP SAP Profile	Displays the default SAP profile for the switch.
Discovery Interval	Displays how often the Automatic Fabric discovery process will run.
Discovery Status	Displays whether the global discovery process is running or idle.
LACP Discovery Status	Displays the global status of Automatic Fabric discovery for the LACP protocol.

output definitions (continued)

LBD Discovery Status	Displays the status of the Loopback Detection on dynamically created UNP Service Access Points (SAPs).
MVRP Discovery Status	Displays the global status of Automatic Fabric discovery for the MVRP protocol.
OSPFv2 Discovery Status	Displays the global status of Automatic Fabric discovery for the OSPFv2 protocol.
OSPFv3 Discovery Status	Displays the global status of Automatic Fabric discovery for the OSPFv3 protocol.
ISIS Discovery Status	Displays the global status of Automatic Fabric discovery for the ISIS protocol.
SPB Discovery Status	Displays the global status of Automatic Fabric discovery for the SPB protocol.

Release History

Release 7.3.2; command introduced.
Release 7.3.4; **OSPFv2 Discovery Status**, **OSPFv3 Discovery status**, **ISIS Discovery Status**, **LBD Discovery Status**, and **Default UNP SAP Profile** output fields added.

Related Commands

auto-fabric admin-state	Enables or disables Automatic Fabric functionality.
auto-fabric config-save admin-state	Configures the status of the Automatic Fabric configuration save timer.
auto-fabric config-save interval	Configures how often the discovered Automatic Fabric configuration is saved to the switch configuration file.
auto-fabric protocols spb default-profile	Configures the default SAP profile for the switch.
auto-fabric discovery-interval	Configures how often the Automatic Fabric discovery process will run.
auto-fabric protocols	Enables or disables Automatic Fabric discovery for specific protocols.

MIB Objects

```
AutoFabTable
   alaAutoFabricGlobalStatus
   alaAutoFabricGlobalDiscovery
   alaAutoFabricGlobalLACPProtocolStatus
   alaAutoFabricGlobalSPBProtocolStatus
   alaAutoFabricGlobalMVRPProtocolStatus
   alaAutoFabricGlobalConfigSaveTimer
   alaAutoFabricGlobalConfigSaveTimerStatus
   alaAutoFabricGlobalDiscoveryTimer
   alaAutoFabricGlobalOSPFv2ProtocolStatus
   alaAutoFabricGlobalOSPFv3ProtocolStatus
   alaAutoFabricGlobalISISProtocolStatus
   alaAutoFabricSPBDefaultProfile
   alaAutoFabricLBDProtocolStatus
```

show auto-fabric config interface

Displays the Automatic Fabric configuration applied on interfaces.

show auto-fabric config interface [*chassis/slot***[-***slot2***] | ***chassis/slot/port***[-***port2***]]**

Syntax Definitions

chassis	The chassis identifier.
*slot***[-***slot2***]**	The slot number. Use a hyphen to specify a range of slot numbers (1/1-5 displays ports on slots 1 through 5).
*slot/port***[-***port2***]**	The chassis ID, slot, and port number. Use a hyphen to specify a range of ports (1/1/2-10 displays ports 1 through 10).

Defaults

By default, the Automatic Fabric configuration for all switch ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

To display the global and port-level configuration for specific interfaces, specify a port number this command.

Examples

```
->show auto-fabric config interface

  Port   Admin Status   LACP      SPB-M      MVRP      SAP Profile    Oper Status
--------+------------+---------+----------+---------+---------------+--------------
 1/1/1   disabled     enabled   enabled    disabled  single-service  disabled
 1/1/2   enabled      enabled   enabled    disabled  auto-vlan       disabled
 1/1/3   enabled      enabled   enabled    enabled   auto-vlan       disabled
 1/1/4   enabled      enabled   disabled   enabled   auto-vlan       disabled
 1/1/5   enabled      enabled   enabled    enabled   auto-vlan       disabled
 1/1/6   enabled      enabled   enabled    enabled   auto-vlan       disabled
```

output definitions

Port	The chassis ID, slot, and port number.
Admin-Status	The Automatic Fabric administrative status for the port.
LACP	The LACP discovery status for the port.
SPB-M	The SPB-M discovery status for the port.
MVRP	The MVRP discovery status for the port.
SAP Profile	The default SAP profile assigned to the port.
Operational Status	The Automatic Fabric operational status for the port.

```
-> show auto-fabric config interface 1/1/1
Auto-Fabric Interface Config:
    Port 1/1/1:
      Operational Status : Disabled
        Admin-Status
          Global : Disabled,   Port : Disabled
        LACP
          Global : Enabled,    Port : Enabled
        SPB-M
          Global : Enabled,    Port : Enabled
        MVRP
          Global : Enabled,    Port : Disabled
        SAP Profile
          Global : Auto-vlan,      Port : Single-service
```

output definitions

Port	The chassis ID, slot, and port number.
Operational Status	The Automatic Fabric operational status.
Admin-Status	The global and port-level administrative status for Automatic Fabric.
LACP	The global and port-level discovery status for LACP.
SPB-M	The global and port-level discovery status for SPB-M.
MVRP	The global and port-level discovery status for MVRP.
SAP Profile	The global SAP profile and port-level SAP profile.

Release History

Release 7.3.2; command introduced.
Release 7.3.4; **SAP Profile** and **Operational status** output fields added.

Related Commands

auto-fabric admin-state	Enables or disables Automatic Fabric functionality.
auto-fabric protocols	Enables or disables the Automatic Fabric discovery process for a particular protocol.
auto-fabric protocols spb default-profile	Configures the default SAP profile for the switch.
auto-fabric protocols spb set-profile	Configures the default SAP profile for a specific port or range of ports.

MIB Objects

```
   alaAutoFabricGlobalStatus
   alaAutoFabricGlobalLACPProtocolStatus
   alaAutoFabricGlobalSPBProtocolStatus
   alaAutoFabricGlobalMVRPProtocolStatus
alaAutoFabricPortConfigTable
   alaAutoFabricPortConfigIfIndex
   alaAutoFabricPortConfigStatus
   alaAutoFabricPortLACPProtocolStatus
   alaAutoFabricPortSPBProtocolStatus
   alaAutoFabricPortMVRPProtocolStatus
   alaAutoFabricPortStatus
   alaAutoFabricPortSPBDefaultProfile
```

19 IP Commands

This chapter details Internet Protocol (IP) commands for the switch. IP is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be forwarded. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols.

IP is enabled on the switch by default and there are few options that can, or need to be, configured. This chapter provides instructions for basic IP configuration commands. It also includes commands for several Layer 3 and Layer 4 protocols that are associated with IP:

- Address Resolution Protocol (ARP)—Used to match the IP address of a device with its physical (MAC) address.
- Internet Control Message Protocol (ICMP)—Specifies the generation of error messages, test packets, and informational messages related to IP. ICMP supports the **ping** command that is used to determine if hosts are online.
- Transmission Control Protocol (TCP)—A major data transport mechanism that provides reliable, connection-oriented, full-duplex data streams. While the role of TCP is to add reliability to IP, TCP relies upon IP to do the actual delivering of datagrams.
- User Datagram Protocol (UDP)—A secondary transport-layer protocol that uses IP for delivery. UDP is not connection-oriented and does not provide reliable end-to-end delivery of datagrams. But some applications can safely use UDP to send datagrams that do not require the extra overhead added by TCP.

The IP commands also include protection from Denial of Service (DoS) attacks. The goal of this feature is to protect a switch from well-known DoS attacks and to notify the administrator or manager when an attack is underway. Also, notifications can be sent when port scans are being performed.

Note. If all devices are on the same VLAN or if the IP interfaces are created on multiple VLANs to enable routing of packets, packets can be forwarded using IP. However, IP routing requires one of the IP routing protocols: Routing Information Protocol (RIP) or Open Shortest Path First (OSPF). See the following chapters for the appropriate CLI commands: Chapter 19, “IP Commands,” Chapter 26, “OSPF Commands.” For more information on VLANs and RIP, see the applicable chapters in the Configuration Guide. For more information on OSPF, see the “Configuring OSPF” chapter in the *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide*.

MIB information for the IP commands is as follows:

Filename: IP-FORWARD-MIB.mib
Module: ipForward

Filename: IP-MIB.mib
Module: ipMIB

Filename: ALCATEL-IND1-IP-MIB.mib
Module: alcatelIND1IPMIB

Filename: ALCATEL-IND1-IPRM-MIB.mib
Module: alcatelIND1IPRMMIB

A summary of the available commands is listed here:

IP	**ip interface** **ip interface rtr-port** **ip interface tunnel** **ip interface dhcp-client** **ip router primary-address** **ip router router-id** **ip static-route** **ip static-route all bfd-state** **ip static-route bfd-state** **ip route-pref** **ip default-ttl** **ping** **traceroute** **ip directed-broadcast** **ip directed-broadcast trusted-source-ip** **ip directed-broadcast clear** **show ip directed-broadcast** **ip service** **ip service port** **ip service source-ip** **show ip traffic** **show ip interface** **show ip emp-interfaces** **show ip routes** **show ip route-pref** **show ip redist** **show ip access-list** **show ip route-map** **show ip router database** **show ip emp-routes** **show ip config** **show ip protocols** **show ip router-id** **show ip service** **show ip service source-ip**

IP Route Map Redistribution	**ip redist** **ip access-list** **ip access-list address** **ip route-map action** **ip route-map match ip address** **ip route-map match ipv6 address** **ip route-map match ip-nexthop** **ip route-map match ipv6-nexthop** **ip route-map match tag** **ip route-map match ipv4-interface** **ip route-map match ipv6-interface** **ip route-map match metric** **ip route-map match route-type** **ip route-map match protocol** **ip route-map match name** **ip route-map set metric** **ip route-map set metric-type** **ip route-map set tag** **ip route-map set community** **ip route-map set local-preference** **ip route-map set level** **ip route-map set ip-nexthop** **ip route-map set ipv6-nexthop** **show ip redist** **show ip access-list** **show ip route-map**
Multiple Virtual Routing and Forwarding (VRF)	**vrf** **show vrf** **show vrf-profiles**
Route Leak	**ip export** **ip import** **show ip export** **show ip import** **show ip global-route-table**
ARP	**arp** **ip distributed-arp admin-state** **clear arp-cache** **ip dos arp-poison restricted-address** **arp filter** **clear arp filter** **show arp** **show ip dos arp-poison** **show ip arp utilization** **show arp filter**
ICMP	**icmp type** **icmp unreachable** **icmp echo** **icmp timestamp** **icmp addr-mask** **icmp messages** **show icmp control** **show icmp statistics**
TCP	**ip tcp half-open-timeout** **show tcp statistics** **show tcp ports** **show ip tcp half-open-timeout**

UDP	**show udp statistics** **show udp ports**
Denial of Service (DoS)	**ip dos scan close-port-penalty** **ip dos scan tcp open-port-penalty** **ip dos scan udp open-port-penalty** **ip dos scan threshold** **ip dos trap** **ip dos scan decay** **ip dos type** **show ip dos config** **show ip dos statistics**

ip interface

Configures an IP interface to enable IP routing on a VLAN or allow remote access. Without an IP interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

ip interface {*if_name* | **emp | master emp | local chassis-id** *chassis***} [{address | vip-address}** *ip_address***] [mask** *subnet_mask***] [admin-state [enable | disable]] [vlan** *vlan_id* | **service** *service_id***] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [e2 | snap] [primary | no primary]**

no ip interface *if_name*

Syntax Definitions

if_name	Text string of the interface name. Use quotes around string if description contains multiple words with spaces between them (for example, "ALE Marketing"). This value is case sensitive.
emp	Modifies the shared EMP port IP address.
master emp	Modifies the EMP port IP address of the master chassis when operating in virtual chassis mode.
local chassis-id *chassis*	Modifies the EMP port IP address of the local chassis.
address *ip_address*	An IP host address (for example, 10.0.0.1, 171.15.0.20) to specify the IP router network.
vip-address *ip_address*	An IP host address for a Virtual IP (VIP) VLAN.
subnet_mask	A valid IP address mask (for example, 255.0.0.0, 255.255.0.0) to identify the IP subnet for the interface.
enable	Enables the administrative status for the IP interface.
disable	Disables the administrative status for the IP interface.
vlan_id	An existing VLAN ID number (1–4094).
service_id	An existing Shortest Path Bridging (SPB) or L2 GRE tunneling service ID number (1–32767). *This parameter is supported only on the OmniSwitch 9900.*
forward	Enables forwarding of IP frames to other subnets.
no forward	Disables forwarding of IP frames. The router interface still receives frames from other hosts on the same subnet.
local-proxy-arp	Enables Local Proxy ARP on the specified interface.
no local-proxy-arp	Disables Local Proxy ARP on the specified interface.
e2	Enter **e2** or **ethernet2** to specify Ethernet-II encapsulation.
snap	SNAP encapsulation.
primary	Designates the specified IP interface as the primary interface for the VLAN.
no primary	Removes the configured primary IP interface designation for the VLAN. The first interface bound to the VLAN becomes the primary by default.

Defaults

parameter	default
ip_address	0.0.0.0
subnet_mask	IP address class
enable | disable	**enable**
vlan_id | *service_id*	none (unbound)
forward | no forward	**forward**
local-proxy-arp | no local-proxy-arp	**no local-proxy-arp**
e2 | snap	**e2**
primary | no primary	First interface bound to a VLAN.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IP interface.
- IP multinetting is supported on VLANs. As a result, it is possible to configure up to 16 IP interfaces per VLAN. Each interface is configured with a different subnet, thus allowing traffic from each configured subnet to coexist on the same VLAN.
- When local proxy ARP is enabled for any one IP router interface associated with a VLAN, the feature is applied to the entire VLAN. It is not necessary to enable it for each interface. However, if the IP interface that has this feature enabled is moved to another VLAN, Local Proxy ARP is enabled for the new VLAN and must be enabled on another interface for the old VLAN.
- When Local Proxy ARP is enabled, all traffic is routed instead of bridged within the VLAN. ARP requests return the MAC address of the IP router interface. The same MAC address is assigned to each interface configured for a VLAN.
- Local Proxy ARP takes precedence over any switch-wide ARP or Proxy ARP function. It is not necessary to have Proxy ARP configured to use Local Proxy ARP. The two features are independent of each other.
- By default, the first interface bound to a VLAN becomes the primary interface for that VLAN. Use the **primary** keyword with this command to configure a different IP interface as the primary. Note that this option is not supported with interfaces bound to an SPB service, as multinetting is not supported on a service. There is only one IP interface per service allowed.
- To create an IP interface for network management purposes, specify **Loopback0** (case sensitive) as the name of the interface. The Loopback0 interface is not bound to any VLAN, so it always remains operationally active.
- Specify the **service** parameter to create a service-based interface that is used to provide in-line routing for SPB and L2 GRE tunneling services. When creating an IP interface for an SPB service or an L2 GRE tunneling service, consider the following:
  - The service ID specified must already exist in the switch configuration.

  - VLAN translation is automatically enabled when a service is assigned to an IP interface regardless of whether or not VLAN translation is enabled for the service; the VLAN translation status is no longer configurable as long as the service is bound to an IP interface.
  - Mixing switches with VLAN translation enabled on some and disabled on other switches in the same network is not recommended. Make sure all switches have VLAN translation enabled, especially if an OmniSwitch 9900 with a service-based interface is added to the network.
  - The same SPB service ID can be assigned to an IPv4 and an IPv6 interface as long as both interface types are in the same VRF instance.
  - See the “IP over SPBM” section in the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information.
  - See the “Using L2 GRE Tunneling” section in the “Configuring Access Guardian” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information.

- Configure an IP interface on the Control BVLAN to support in-band management access in the SPBM domain. When creating an IP interface on a Control BVLAN, consider the following:
  - The IP interface must be configured only on the Control BVLAN. Only IPv4 interface is supported.
  - Only one Control BVLAN can be configured on a switch. This IP interface will be considered operationally active when the underlying Control BVLAN becomes operationally up and all underlying configuration is considered valid.
  - Whenever the IP interface is operationally down due to an unsupported configuration, the **show ip interface** command will display "Operational State Reason" as “invalid-config”.
  - ISIS-SPB is the only protocol supported in the IP BVLAN domain for exchanging or advertising IP routing information. No other routing protocol (including VRRP) is supported.
  - Multi-netting of IP interfaces on a BVLAN is not supported. Only one IP interface must be configured on the Control BVLAN.
  - STP is not allowed on BVLANs, and all broadcast packets will be restricted on this IP interface. Hence, explicit ARP/ND resolution is not supported. ISIS-SPB will provide the MAC-to-IP address mappings, to avoid broadcast packets in the SPBM backbone domain.
  - The ARPs learned with ISIS SPB on the Control BVLAN will be shown as static ARPs, but these ARPs will have bit "M" (Managed ARP) set in the ARP flags, and displayed as “M” in the “Flags” field of the **show arp** command display.
  - Static routing is required to route packets to destinations outside of the IP BVLAN subnet. Dynamic routing protocols are not supported on this IP interface.
  - The IP BVLAN domain will operate in IP unicast mode, hence IP Multicast is not supported.
  - SPB in-band management is supported on the OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900, and OmniSwitch 9900.
  - See the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information.

Examples

```
-> ip interface Marketing
-> vrf 100 ip interface “Payroll address” 18.12.6.3 vlan 255
-> ip interface “Human Resources” 10.200.12.101 vlan 500 no forward snap
-> ip interface Distribution 11.255.14.102 vlan 500 local-proxy-arp primary
-> no ip interface Marketing
-> vrf 100 no ip interface “Payroll address”

-> ip interface l3-vpn address 10.1.1.1/24 service 10
-> service 10 vlan-xlation disable
ERROR: Modify vlan translation currently not allowed for service (10)
-> vrf 100 ip interface l3-vpn100 address 100.1.1.1/24 service 20
```

```
-> no ip interface l3-vpn
-> vrf 100 no ip interface l3-vpn100
```

Release History

Release 7.1.1; command introduced
Release 8.4.1.R03; **service** parameter added to support binding an SPB service to an IP interface.
Release 8.5R4; **service** parameter support for binding an L2 GRE tunneling service to an IP interface added. Support for an IP interface on an SPB Control BVLAN added.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceVipAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   alaIpInterfaceServiceID
   alaIpInterfaceIpForward
   alaIpInterfaceEncap
   alaIpInterfaceLocalProxyArp
   alaIpInterfacePrimCfg
   alaIpInterfaceOperState
   alaIpInterfaceOperReason
   alaIpInterfaceRouterMac
   alaIpInterfaceBcastAddr
   alaIpInterfacePrimAct
```

ip interface rtr-port

Configures an IP routed-port interface by associating an IP interface with a port or link aggregate and a VLAN.

ip interface *if_name* **address** *ip_address/mask* **vlan** *vlan_id* **rtr-port {port** *chassis/slot/port* **| linkagg** *agg_id***} {tagged | untagged}**

Syntax Definitions

if_name	A unique name for the IP interface. Use quotes around the string if the name contains multiple words with spaces between them (for example, “ALE Marketing”). This value is case sensitive.
ip_address	IP host address to specify this IP interface.
mask	IP mask to specify this IP interface.
vlan_id	An unused VLAN ID to which this IP interface is associated.
chassis/slot/port	The chassis, slot, and port number (1/1/3) of the physical port to bind to the IP interface.
agg_id	The link aggregate ID to bind to the IP interface.
tagged	Whether the assigned port or link aggregate is tagged for the specified VLAN.
untagged	Whether the assigned port or link aggregate is untagged for the specified VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- In a single step, this command creates the specified VLAN, configures an IP interface for the VLAN, and assigns a port or link aggregate (tagged or untagged) to the VLAN.
- Configuring an IPv4 and IPv6 routed-port interface for the same VLAN ID is supported if the following conditions are met:
  - The VLAN ID, port, and the tagged/untagged port status for both interfaces is the same (for example, IPv4 and IPv6 routed interfaces are both bound to VLAN 850 with port 1/1/2 tagged).
  - Both interfaces are configured in the same VRF instance.
- Make sure the specified VLAN ID does not already exist in the switch configuration or is only used as a routed-port VLAN for an IPv4 interface. This VLAN will serve as a routing-only VLAN with a single port or link aggregate (Layer 2 functionality is not supported).
- Make sure the specified port or link aggregate is not already assigned to a VLAN that is *not* a routed-port VLAN. However, the port or link aggregate can be assigned to other routed-port VLANs.

- Attempting to add more ports or link aggregates to the routed-port VLAN or attempting to delete the VLAN is not allowed. The VLAN can only be removed by deleting the associated IPv4 and, if configured, the associated IPv6 interface.
- The same VLAN cannot be used for both a routed-port interface and a non-routed-port interface.
- Once configured, an IP routed-port interface is operationally equivalent to an IP VLAN interface. Routing protocols and other switch features that use IP are configured and operate on an IP routed-port interface in the same manner as on a regular IP interface.

Examples

```
-> ip interface “rp-vlan30” 10.0.0.1/8 vlan 30 rtr-port port 1/1/1 tagged
-> ip interface “rp-vlan40” 20.0.0.1/8 vlan 40 rtr-port port 1/1/2 untagged
-> ip interface “rp-vlan50” 30.0.0.1/8 vlan 40 rtr-port linkagg 6 tagged
-> ip interface “rp-vlan60” 40.0.0.1/8 vlan 50 rtr-port linkagg 7 untagged

-> vlan 70
-> ip interface rp-vlan70 rtr-port port 1/1/13 untagged vlan 70
ERROR: vlan 70 already present

-> ip interface rpv4-vlan rtr-port port 1/1/11 tagged vlan 300
-> ipv6 interface rpv6-vlan rtr-port port 1/1/11 tagged vlan 300

-> no ipv6 interface rpv6-vlan
-> ipv6 interface rpv6-vlan rtr-port port 1/1/13 untagged vlan 300
ERROR: Configuration conflict with IPv4 routed port interface rpv4-vlan
```

Release History

Release 7.3.4; command introduced

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceVlanID
   alaIpInterfaceDeviceType
   alaIpInterfacePortIfindex
   alaIpInterfaceTag
```

ip interface tunnel

Configures the end points for a GRE or IPIP tunnel.

ip interface *if_name* **tunnel [source** *ip_address***] [destination** *ip_address***] [protocol {ipip | gre}]**

Syntax Definitions

if_name	Text string. Use quotes around string if description contains multiple words with spaces between them (for example, “ALE Marketing”). This value is case sensitive.
source *ip_address*	Source IP address of the tunnel.
destination *ip_address*	Destination IP address of the tunnel.
ipip	Specifies the tunneling protocol as IPIP.
gre	Specifies the tunneling protocol as GRE.

Defaults

parameter	default
ipip | gre	**ipip**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

You can configure an interface as either a VLAN or tunnel interface.

Examples

```
-> ip interface “tnl-1” tunnel source 23.23.23.1 destination 155.2.2.2 protocol gre
-> ip interface “tnl-1” tunnel source 23.23.23.1 destination 155.2.2.2 protocol
ipip
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceTunnelSrc
   alaIpInterfaceTunnelDst
   alaIpInterfaceDeviceType
```

ip interface dhcp-client

Configures a DHCP client IP interface that is to be assigned an IP address from a DHCP server.

ip interface dhcp-client [vlan *vlan_id* **] [vsi-accept-filter** *filter-string* **| server-preference] [release | renew] [option-60** *opt60_string***] [admin {enable | disable}] [local-proxy-arp | no local-proxy-arp]]**

no ip interface dhcp-client

ip interface dhcp-client no server-preference

Syntax Definitions

dhcp-client	Reserved IP interface name indicating this interface use DHCP to obtain an IP address from a DHCP server.
vlan_id	An existing VLAN ID number (1–4094).
filter-string	String that matches with option-43 filed of the DHCPACK to prefer the desired OXO server. By default the filter-string will be empty string (“ “).
server-preference	Enables DHCP server precedence logic. The DHCP server preference logic is mutually exclusive with vsi-accept-filter.
release	Releases the DHCP server assigned IP address.
renew	Renews the DHCP server assigned IP address.
opt60_string	The option-60 field value to be included in DHCP discover/request packets.
enable	Enables the administrative status for the IP interface.
disable	Disables the administrative status for the IP interface.
local-proxy-arp	Enables Local Proxy ARP on the specified interface.
no local-proxy-arp	Disables Local Proxy ARP on the specified interface.

Defaults

parameter	default
opt60_string	OmniSwitch-xxxx (xxxx = Platform, for example, 6900)
enable | disable	enable
filter-string	(“ “).
server-preference	disabled
local-proxy-arp | no local-proxy-arp	**no local-proxy-arp**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the DHCP-client IP interface.
- Only one DHCP client IP interface can be assigned per switch but it can belong to any VLAN and any VRF instance.
- If the system name has not been configured, it will be updated using the option-12 field. If the option-12 string is greater than 19 characters the remaining characters will be truncated.
- The minimum lease time accepted on the DHCP-client interface is 5 minutes.
- The VSI filter-string once configured cannot be deleted. It can be overwritten or modified. It can be configured as empty string (“ “).
- The VSI accept filter is case-sensitive. The maximum length of a vsi-accept-filter can be of 64 character length.
- In order to retain the same OXO server which was configured before RCL, the VSI filter must match the hard coded string “alcatel.a4400.0”.
- DHCP client preference to obtain the lease from the highest priority server among the multiple offers received can be enabled using the **server-preference** option.
- Server preference option can also be set without specifying VLAN ID, provided the dhcp-client interface is associated with a VLAN prior to setting the server preference.
- The **server-preference** option is mutually exclusive with **vsi-accept-filter** option.
- Use the **no server-preference** option to remove the server preference.

Examples

```
-> ip interface dhcp-client vlan 100
-> ip interface dhcp-client admin enable
-> ip interface dhcp-client release
-> ip interface dhcp-client renew
-> ip interface dhcp-client option-60 OmniSwitch
-> no ip interface dhcp-client
-> ip interface dhcp-client vsi-accept-filter “alcatel.a4400.0”
-> ip interface dhcp-client vlan 1 server-preference
-> ip interface dhcp-client server-preference
-> ip interface dhcp-client no server-preference
```

Release History

Release 7.3.4; command introduced.
Release 8.5R1; **server-preference** parameters included.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceDhcpStatus
   alaIpInterfaceDhcpIpRelease
   alaIpInterfaceDhcpIpRenew
   alaIpInterfaceDhcpOption60String
   alaIpInterfaceDhcpVsiAcceptFilterString
   alaIpInterfaceDhcpServerPreference
```

ip router primary-address

Configures the router primary IP address. By default, the router primary address is derived from the first IP interface that becomes operational on the router.

ip router primary-address *ip_address*

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The router primary address must be a valid IP unicast host address.
- The router primary IP address is used by BGP to derive its unique BGP Identifier, if the router router-id is not a valid IP unicast address.
- It is recommended that the primary address be explicitly configured on dual CMM chassis.

Examples

```
-> ip router primary-address 172.22.2.115
```

Release History

Release 7.1.1; command introduced

Related Commands

ip router router-id	Configures the router ID for the router.

MIB Objects

```
alaDcrTmConfig
   alaDrcTmIpRouterPrimaryAddress
```

ip router router-id

Configures the router ID for the router. By default, the router primary address of the router is used as the router ID. However, if a primary address has not been explicitly configured, the router ID defaults to the address of the first IP interface that becomes operational.

ip router router-id *ip_address*

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The router ID can be any 32-bit number.
- If the router ID is not a valid IP unicast host address, the BGP identifier is derived from the router primary address.
- It is recommended that the router ID be explicitly configured on dual CMM chassis.
- The router ID is used by OSPF and BGP for unique identification of the router in the network.

Examples

```
-> ip router router-id 172.22.2.115
```

Release History

Release 7.1.1; command introduced

Related Commands

ip interface dhcp-client	Configures the router primary IP address.

MIB Objects

```
alaDcrTmConfig
   alaDrcTmIpRouterId
```

ip static-route

Creates or deletes an IP static route. Static routes are user-defined; they carry a higher priority than routes created by dynamic routing protocols. By default, static routes carry a higher priority than the dynamic routes.

ip static-route *ip_address* **[mask** *mask***] {gateway {***gateway_address* **| null} [tag** *num***] [name** *string***] | interface** *interface_name* | **follows** *ip_address***} [metric** *metric***]**

no ip static-route *ip_address* **[mask** *mask***] [gateway {***gateway_address* **| null**} **| interface** *interface_name* | **follows** *ip_address***] [metric** *metric***]**

Syntax Definitions

ip_address	Destination IP address of the static route.
mask	Subnet mask corresponding to the destination IP address.
gateway *gateway_address*	IP address of the next hop used to reach the destination IP address.
gateway null	Use this option to configure an IPv4 blackhole route.
tag *num*	Tag to be used for route.
name *string*	Name to be used for route.
interface *interface _name*	Interface of the next hop used to reach the destination IP address.
follows *ip_address*	The recursive static route follows this IP address. The recursive route uses the same gateway (and interface) or nexthop that is used to reach this host address.
metric	Metric or cost (hop count) for the static route. You can set a priority for the static route by assigning a metric value. The lower the metric value, the higher the priority. Valid range is 1–15.

Defaults

parameter	default
metric	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- By default, static routes have a higher priority over dynamic routes; however, it can be changed using the **ip route-pref** command.
- Static routes do not age out of the routing tables; however, they can be deleted. Use the **no** form of this command to delete a static route.
- A static route is active if the interface it is using is “UP”.
- The subnet mask is not required if you want to use the natural subnet mask. By default, the switch imposes a natural mask on the IP address.

- If directly connected, NAT routers interface name can be used instead of gateway IP address, provided the router is enabled for proxy-ARP to handle ARP requests for the route addresses.
- Use the **null** option to configure IPv4 blackhole routes. A blackhole route is used to forward unwanted traffic to a blackhole.
  - Redistribution of blackhole routes is supported. Dynamic routing protocols may advertise these routes, but the gateway associated with the route(s) will be an address on the router advertising them.
  - Leaking of blackhole routes across SPB service backbones is supported. However, blackhole routes cannot be leaked between VRFs. Blackhole routes need to be explicitly configured using the **ip static-route** command in any/all VRFs.
  - Blackhole routes are created and installed through static route commands. Dynamic Routing protocols shall not install blackhole IP routes.
  - Blackhole routes shall never be part of ECMP.
  - Blackhole routes cannot be enabled for BFD support.
- Alternatively, the gateway address '0.0.0.0' can be used to create an IPv4 blackhole route.

Examples

```
-> ip static-route 171.11.1.0/24 gateway 171.11.2.1
-> ip static-route 171.11.1.0/24 interface Int1
-> ip static-route 12.0.0.0/8 interface Int1
-> ip static-route 171.11.1.0/24 follows 192.168.10.1
-> ip static-route 55.0.0.0/8 gateway null
-> ip static-route 55.0.0.0/8 gateway 0.0.0.0
```

Release History

Release 7.1.1; command introduced
Release 7.3.4; **interface, tag, name** parameters included
Release 8.6R1; **null** keyword added.

Related Commands

ip route-pref	Configures the route preference of a router.
show ip routes	Displays the IP Forwarding table.
show ip router database	Displays a list of all routes (static and dynamic) that exist in the IP router database.
show ip route-pref	Displays the IPv4 routing preferences of a router.

MIB Objects

```
alaIprmStaticRoute
   alaIprmStaticRouteDest
   alaIprmStaticRouteMask
   alaIprmStaticRouteNextHop
   alaIprmStaticRouteTag
   alaIprmStaticRouteName
   alaIprmStaticRouteMetric
   alaIprmStaticRouteStatus
   alaIprmStaticRouteType
```

ip static-route all bfd-state

Enables BFD for all IPv4 static routes.

ip static-route all bfd-state {enable| disable}

Syntax Definitions

enable	Enables BFD for all IPv4 static routes.
disable	Disables BFD for all IPv4 static routes.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When there are static routes configured in the switch, BFD is enabled to track the gateway.
- If the route is not reachable, it will be moved to the inactive database.

Examples

```
-> ip static-route all bfd-state enable
-> ip static-route all bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip static-route bfd-state	Enables BFD for a specific static route.
show ip router database	Displays a list of all routes (static and dynamic) that exist in the IP router database.

MIB Objects

```
alaIprmConfig
   alaIprmStaticAllBfd
```

ip static-route bfd-state

Enables or disables BFD for a specific IPv4 static route.

ip static-route *ipv4_prefix/pfx_length* **gateway** *ipv4_host_address* **bfd-state {enable| disable}**

Syntax Definitions

ipv4_prefix	The destination IPv4 address.
pfx_length	The prefix length for the destination IP address.
ipv4_host_address	The gateway IPv4 address.
enable	Enables BFD for the IPv4 static route.
disable	Disables BFD for the IPv4 static route.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

BFD is enabled to track the gateway of static routes.

Examples

```
-> ip static-route 192.100.1.0/24 gateway 100.1.1.10 bfd-state enable
-> ip static-route 192.100.1.0/24 gateway 100.1.1.10 bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip static-route all bfd-state	Enables BFD for all static routes.
show ip router database	Displays a list of all routes (static and dynamic) that exist in the IP router database.

MIB Objects

```
alaIprmStaticRouteTable
   alaIprmStaticRouteDest
   alaIprmStaticRouteMask
   alaIprmStaticRouteNextHop
   alaIprmStaticRouteBfdStatus
   alaIprmStaticRouteType
```

ip route-pref

Configures the route preference of a router.

[vrf *vrf_name***] ip route-pref {static | rip | ospf | isisl2 | isisl1 | ibgp | ebgp | import}** *value*

Syntax Definitions

vrf_name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
static	Configures the route preference of static routes.
ospf	Configures the route preference of OSPF routes.
isisl2	Configures the route preference of ISIS L2 routes.
isisl1	Configures the route preference of ISIS L1 routes.
rip	Configures the route preference of RIP routes.
ebgp	Configures the route preference of external BGP routes.
ibgp	Configures the route preference of internal BGP routes.
import	Configures the route preference for the routes that are imported.
value	Route preference value.

Defaults

parameter	default
static *value*	2
ospf *value*	110
isisl2 *value*	118
isisl1 *value*	115
rip *value*	120
ebgp *value*	190
ibgp *value*	200
import *value*	210

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Route preference of local routes cannot be changed.

Examples

```
-> ip route-pref ebgp 20
-> ip route-pref rip 60
-> ip route-pref import 210
```

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** and **import** parameters added.

Related Commands

show ip route-pref	Displays the configured route-preference of a router.
ip import	Configures a route map to import routes from GRT to the destination VRF.
show ip import	Displays the import route configuration details.

MIB Objects

```
alaIprmRtPrefTable
   alaIprmRtPrefEntryType
   alaIprmRtPrefEntryValue
```

ip default-ttl

Configures the Time To Live value (TTL) for IP packets. The TTL value is the maximum number of hops an IP packet travels before being discarded.

ip default-ttl *hops*

Syntax Definitions

hops	TTL value, in hops. Valid range is 1–255.

Defaults

parameter	default
hops	64

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This value represents the default value inserted into the TTL field of the IP header for datagrams originating from this switch whenever a TTL value is not supplied by the transport layer protocol.

Examples

```
-> ip default-ttl 30
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip config	Displays IP configuration parameters.

MIB Objects

```
IpDefaultTTL
```

ping

Tests whether an IP destination can be reached from the local switch. This command sends an ICMP echo request to a destination and then waits for a reply. To ping a destination, enter the **ping** command and enter either the IP address or hostname of the destination. The switch pings the destination using the default frame count, packet size, interval, and timeout parameters (6 frames, 64 bytes, 1 second, and 5 seconds respectively). You can also customize any or all of these parameters as described below.

ping {*ip_address* | *hostname***} [source-interface** *ip_interface***] [count** *count***] [size** *packet_size***] [interval** *seconds***] [timeout** *seconds***] [data-pattern** *string***] [dont-fragment] [tos** *tos_val***]**

Syntax Definitions

ip_address	IPv4 address of the system to ping.
hostname	DNS name of the system to ping.
source-interface *ip_interface*	IP address or interface name to use as the source IP for the ping packets.
count	Number of frames to be transmitted.
packet_size	Size of the data portion of the packet sent for this ping, in bytes. Valid range is 1–65507.
interval *seconds*	Polling interval. The switch polls the host at time intervals specified in seconds.
timeout *seconds*	Number of seconds the program waits for a response before timing out.
data-pattern *string*	The data pattern to be used in the data field of the ping packets.
dont-fragment	Sets the don't-fragment bit in the IP packet.
tos *tos_val*	Type of Service field in the IP header.

Defaults

parameter	default
count	6
packet_size	64
interval *seconds*	1
timeout *seconds*	5
dont-fragment	0
tos *tos_val*	0
data-pattern *string*	Repeating sequence of ASCII characters 0x4 onwards to 0xff

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If you change the default values, they are only applied to the current ping. The next time you use the ping command, the default values are used unless you again enter different values.

Examples

```
-> ping 10.255.11.242

PING 10.255.11.242: 56 data bytes
64 bytes from 10.255.11.242: icmp_seq=0. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=1. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=2. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=3. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=4. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=5. time=0. ms
----10.255.11.242 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0

-> ping 10.0.0.1 source-interface mgmt
-> ping 10.0.0.1 tos 1
-> ping 10.0.0.1 timeout 10
-> ping 10.0.0.1 interval 10
-> ping 10.0.0.1 dont-fragment
-> ping 10.0.0.1 data-pattern AB
```

Release History

Release 7.1.1; command introduced

Related Commands

traceroute	Finds the path taken by an IP packet from the local switch to a specified destination.

MIB Objects

N/A

traceroute

Finds the path taken by an IP packet from the local switch to a specified destination. This command displays the individual hops to the destination as well as some timing information.

traceroute {*ip_address* | *hostname***} [max-hop** *max_hop_count***] [min-hop** *min_hop_count***] [source-interface** *ip_interface***] [probes** *probe_count***] [timeout** *seconds***] [port** *port_number_value***]**

Syntax Definitions

ip_address	IPv4 address of the host whose route you want to trace.
hostname	DNS name of the host whose route you want to trace.
max_hop_count	Maximum hop count for the trace. The valid range is 1–255.
min_hop_count	Minimum hop count for the trace. The valid range is 1–30.
ip_interface	Source IP interface to be used in the traceroute packets.
probe_count	The number of packets (retry) sent for each hop-count. The valid range is 1–10000.
seconds	The time to wait for the response of each probe packet.
port_number_value	The destination port number to be used in the probing packets.

Defaults

parameter	default
max-hop *max_hop_count*	30
min-hop *min_hop_count*	1
source-interface *ip_interface*	Outgoing IP interface as per route lookup
probes *probe_count*	3
timeout *seconds*	5
port *port_number_value*	33334

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When using this command, you must enter the name of the destination as part of the command line (either the IP address or host name).

Examples

```
-> traceroute 128.251.17.224

traceroute to 128.251.17.224, 30 hops max, 40 byte packets
 1  10.255.11.254 0 ms  0 ms  0 ms
 2  172.23.0.251 0 ms  16.6667 ms  0 ms
 3  128.251.14.253 0 ms  0 ms  0 ms
 4  128.251.17.224 0 ms  0 ms  0 ms

-> traceroute 128.251.17.224 max-hop 3
traceroute to 128.251.17.224, 3 hops max, 40 byte packets
 1  10.255.11.254 0 ms  0 ms  0 ms
 2  172.23.0.251 16.6667 ms  0 ms  0 ms
 3  128.251.14.253 0 ms  0 ms  0 ms
-> traceroute 10.0.0.1 source-interface mgmt
-> traceroute 10.0.0.1 min-hop 3
-> traceroute 10.0.0.1 probes 3
-> traceroute 10.0.0.1 timeout 10
-> traceroute 10.0.0.1 port-number 1025
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip routes	Displays the IP Forwarding table.

MIB Objects

N/A

ip directed-broadcast

Enables or disables IP directed broadcasts routed through the switch. An IP directed broadcast is an IP datagram that has all zeros or all 1s in the host portion of the destination address. The packet is sent to the broadcast address of a subnet to which the sender is not directly attached.

[vrf *vrf_name***] ip directed-broadcast {enable | disable}**

Syntax Definitions

vrf_name	The name of an existing VRF instance.
enable	Enables IP directed broadcasts.
disable	Disables IP directed broadcasts.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Directed broadcasts are used in denial-of-service attacks. In a DoS attack, a continuous stream of ping requests are sent from a falsified source address to a directed broadcast address. This results in a large stream of replies, which can overload the host of the source address. By default, the switch drops directed broadcasts. Directed broadcasts must not be enabled.
- When IP directed broadcast is enabled, by default, it is enabled on the 'default' VRF.

Examples

```
-> ip directed-broadcast enable
-> ip directed-broadcast disable
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip directed-broadcast	Displays the status of the directed broadcast configuration and trusted source IP address configuration.

MIB Objects

```
alaIpDirectedBroadcast
```

ip directed-broadcast trusted-source-ip

Specify the source IP address, destination IP address and destination VLAN information to broadcast the packets in controlled manner. The specified information is considered as the trusted information to broadcast the packets received from the defined parameters, and the remaining broadcast packets are dropped.

[vrf *vrf_name***] ip directed-broadcast trusted-source-ip {***ip_address/mask* **|** *ip_address* **mask** *subnet_mask***} [destination-ip {***ip_address/mask* **|** *ip_address* **destination-mask** *subnet_mask***] | destination-vlan {***vlan_id* | *vlan_id[-vlan_id***}]**

[vrf *vrf_name***] no ip directed-broadcast trusted source-ip** *ip_address* **{***ip_address/mask* **|** *ip_address* **mask** *subnet_mask***}**

Syntax Definitions

vrf_name	The name of an existing VRF instance.
trusted-source-ip *ip_address*	Source IP address from which the broadcast packets are received.
destination-ip *ip_address*	Destination address to which the packets must be directed.
subnet_mask	The source mask from which the broadcast packets are received.
destination-mask *subnet_mask*	The destination mask to which the packets must be directed.
vlan_id	Existing VLAN ID to which the packets are to be directed.

Defaults

parameter	default
ip_address	0.0.0.0
subnet_mask	IP address class/0.0.0.0
vlan_id	None

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** command to remove the trusted information configured with the source IP address for controlled IP directed broadcast.
- IP directed broadcast must be enabled for the controlled IP directed broadcast to work.
- When controlled IP directed broadcast is enabled, by default, it is enabled on the ‘default’ VRF.
- The trusted information must have the source IP with optional destination IP address or VLAN ID.
- Ensure that the configured address/mask combination (source/destination IP address) configuration is not a subset of an already existing address/mask.
- If the source IP matches, then the packets are broadcasted in the particular destination IP interface or VLAN interfaces. The remaining packets are dropped.

- When the packet received matches with the source IP and if the destination IP or destination VLAN information are not defined by the user, then the packet will be forwarded based on the routing information in the switch.
- If no source IP is provided as trusted, by default, all the packets are forwarded.
- If the destination IP or VLAN is defined by the user, then the destination address of the packet will be matched with the user defined list and routes the packets if the destination IP matches. If the VLAN information is defined, then the packets will be routed if the destination VLAN matches a VLAN in the configured allowed VLAN list. If neither the destination IP or VLAN matches the ones configured, the packet are dropped.
- If the destination IP is not reachable or if the destination subnet is not directly connected, packet will be dropped.
- If the directed broadcast is set to controlled mode and the user does not specify any trusted information, all the broadcast packets will be dropped. This case is equivalent to disabled state of directed-broadcast.
- 32 source IP addresses can be defined, and each source IP address can have 30 destination IP addresses and 30 destination VLAN IDs.
- If IP directed broadcasts is disabled using the command **ip directed-broadcast disable**, which also is the default, all packets with subnet broadcast, will be dropped.

Examples

```
-> ip directed-broadcast trusted-source-ip 30.0.0.0 mask 255.255.255.0

-> vrf test123 ip directed-broadcast trusted-source-ip 30.0.0.0 mask 255.255.255.0
destination-ip 10.0.0.255 destination-mask 255.255.255.255

-> ip directed-broadcast trusted-source-ip 30.0.0.0/24 destination-ip 10.0.0.255/24

-> ip directed-broadcast trusted-source-ip 30.0.0.0 mask 255.255.255.0
destination-vlan 10

-> ip directed-broadcast trusted-source-ip 30.0.0.0/24 destination-vlan 10-15

-> no ip directed-broadcast trusted-source-ip 30.0.0.0/24
-> no ip directed-broadcast trusted-source-ip 30.0.0.0 mask 255.255.255.0
```

Release History

Release 8.5R2; command introduced.

Related Commands

ip directed-broadcast	Enables or disables IP directed broadcasts routed through the switch.
ip directed-broadcast clear	Clears all the trusted information configured.
show ip directed-broadcast	Displays the status of the directed broadcast configuration and trusted source IP address configuration.

MIB Objects

```
alaIpDirectedBroadcastCtrlSrcTable
   alaIpDirectedBroadcastCtrlSrcAddrType
   alaIpDirectedBroadcastCtrlSrcAddr
   alaIpDirectedBroadcastCtrlSrcMask
alaIpDirectedBroadcastCtrlDstTable
   alaIpDirectedBroadcastCtrlDstAddrType
   alaIpDirectedBroadcastCtrlDstAddrType
   alaIpDirectedBroadcastCtrlDstMask
alaIpDirectedBroadcastCtrlVlanTable
   alaIpDirectedBroadcastCtrlVlanID
```

ip directed-broadcast clear

Clears all the trusted information configured.

[vrf *vrf_name***] ip directed-broadcast clear [trusted-source-ip {***ip_address/mask* **|** *ip_address* **mask** *subnet_mask***}]**

Syntax Definitions

vrf_name	The name of an existing VRF instance.
trusted-source-ip *ip_address*	Source IP address from which the broadcast packets are received.
subnet_mask	The source mask from which the broadcast packets are received.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

If the source IP is specified, then the destination and the VLAN information for the source IP specified is cleared. If the command is specified without the source IP address, entire trusted information database is cleared.

Examples

```
-> ip directed-broadcast clear
-> ip directed-broadcast clear trusted-source-ip 20.20.20.0 mask 255.255.255.0
```

Release History

Release 8.5R2; command introduced.

Related Commands

ip directed-broadcast	Enables or disables IP directed broadcasts routed through the switch.
ip directed-broadcast trusted-source-ip	Specify the source IP address, destination IP address and destination VLAN information to broadcast the packets in controlled manner.

MIB Objects

```
alaIpDirectedBroadcastCtrlSrcTable
   alaIpDirectedBroadcastCtrlSrcAddrType
   alaIpDirectedBroadcastCtrlSrcAddr
   alaIpDirectedBroadcastCtrlSrcMask
   alaIpDirectedBroadcastCtrlSrcClear
alaIpDirectedBroadcastCtrlGlobalConfig
   alaIpDirectedBroadcastCtrlClearAll
```

show ip directed-broadcast

Displays the status of the directed broadcast configuration and trusted source IP address configuration.

[vrf *vrf_name***] show ip directed-broadcast [trusted-source-ip {***ip_address/mask* **|** *ip_address* **mask** *subnet_mask***}] details**

Syntax Definitions

vrf_name	The name of an existing VRF instance.
trusted-source-ip *ip_address*	Source IP address from which the broadcast packets are received.
subnet_mask	The source mask from which the broadcast packets are received.
details	Displays the destination IP address or VLAN information for the specified source IP.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use **details** keyword to view the destination IP addresses or VLANs information for the specified source IP.

Examples

```
-> show ip directed-broadcast
IP Directed Broadcast is enabled
Source-IP         MASK              Destination-IP VLAN
------------------+-----------------+--------------+-----
100.10.1.0        255.255.255.0     YES            NO
100.10.2.2        255.255.255.255   YES            NO
100.10.3.0        255.255.255.224   YES            NO
100.10.4.0        255.255.255.248   YES            NO

-> show ip directed-broadcast trusted-source-ip 10.10.10.0 mask 255.255.255.0
details
Source-IP/Mask         =    10.10.10.0/255.255.255.0
Destination-IP/Mask    =    20.20.20.0/255.255.255.0,
Vlan                   =    10
```

output definitions

Source-IP/Mask	Trusted source IP address and mask configured in a controlled manner.
Destination-IP/Mask	Trusted destination IP address and mask configured in a controlled manner.
Vlan	Trusted VLAN ID configured for directed broadcast in a controlled manner.

Release History

Release 8.5R2; command introduced.

Related Commands

ip directed-broadcast	Enables or disables IP directed broadcasts routed through the switch.
ip directed-broadcast trusted-source-ip	Specify the source IP address, destination IP address and destination VLAN information to broadcast the packets in controlled manner.

MIB Objects

N/A

ip service

Enables (opens) or disables (closes) well-known or user-defined TCP/UDP service ports. Selectively enabling or disabling these types of ports provides an additional method for protecting against unauthorized switch access or Denial of Service (DoS) attacks.

[vrf *vrf_name***] ip service {all |** *service_name* | **port** *service_port***} admin-state {enable | disable}**

Syntax Definitions

vrf_name	The name of an existing VRF instance in which services are to be enabled or disabled.
all	Configures access to all TCP/UDP ports.
service_name	The name of the TCP/UDP service to enable or disable. (Refer to the table in the "Usage Guidelines" section for a list of supported service names.)
service_port	A TCP/UDP service port number. Configures access by port number rather than by service name. (Refer to the table in the "Usage Guidelines" section for a list of well-known port numbers.) If a user-defined port number is specified, the valid range is 20000–20999.
enable	Enables access to the service.
disable	Disables access to the service.

Defaults

All TCP/UDP ports are open by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies to TCP/UDP service ports opened by default. It does not affect ports that are opened by applications, such as RIP, BGP, and so on.
- Use the **all** option with this command to configure access to all well-known TCP/UDP service ports.
- To designate which port to enable or disable, specify either the name of a service or the well-known port number associated with that service. Specifying a name and a port number in a single command line is not supported.
- When using service names, it is possible to specify more than one service in a single command line by entering each service name separated by a space. See the "Example" section for more information.
- When specifying a service port number, the **port** keyword is required and that only one port number is allowed in a single command.

- The following table lists the **ip service** command options for specifying TCP/UDP services and also includes the well-known port number associated with each service:

service name	port
ftp	21
ssh	22
telnet	23
http	80
https	443
ntp	123
snmp	161

- If a VRF is specified, the service is enabled or disabled in the specified VRF. By default, the services are enabled in the 'default' VRF.

Examples

```
-> ip service all admin-state disable
-> ip service ftp admin-state enable
-> ip service port 20000 admin-state enable
-> vrf vrf1 ip service ftp admin-state enable
```

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** parameter added.

Related Commands

ip service port	Configures a user-defined TCP/UDP port for the specified service.
show ip service	Displays the IP service TCP/UDP port configuration and status.

MIB Objects

```
alaIpServiceTable
   alaIpServiceType
   alaIpServicePort
   alaIpServiceStatus
alaIpPortServiceTable
   alaIpPortServicePort
   alaIpPortServiceStatus
```

ip service port

Configures a user-defined TCP/UDP service port for the specified service.

ip service {*service_name***} port {default |** *service_port***}**

Syntax Definitions

service_name	The name of the TCP/UDP service to enable or disable. (Refer to the table in the "Usage Guidelines" section for a list of supported service names.)
service_port	A TCP/UDP service port number (Refer to the table in the "Usage Guidelines" section for a list of supported service names.) Valid range is the default service port number or 20000-20999.
default	Sets the port back to the well-known port for the specified service.

Defaults

By default, the service uses the well-known TCP/UDP port number for that service.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **default** parameter with this command to set the port for the specified service back to the well-known default port for that service. For example, if the FTP port was previously changed to "20000", then the **ip service ftp port default** command would set the FTP port back to "21".
- The following table lists the **ip service port** command options for specifying TCP/UDP services and also includes the default well-known port number associated with each service:

service name	port
ftp	21
ssh	22
telnet	23
http	80
https	443

  The **ntp** and **snmp** services are not supported with the **ip service port** command.
- Use the **ip service** command to enable or disable the status for a well-known or user-defined TCP/UDP service port.

Examples

```
-> ip service ftp port 20000
-> ip service ftp port default
-> ip service telnet port 20003
```

```
-> ip service telnet port default
```

Release History

Release 7.1.1; command introduced

Related Commands

ip service	Enables or disables well-known or user-defined service ports.
show ip service	Displays the IP service TCP/UDP port configuration and status.

MIB Objects

```
alaIpServiceTable
   alaIpServiceType
   alaIpServicePort
   alaIpServiceStatus
```

ip service source-ip

Configures a user-defined source IP address as the outgoing IP interface for the IP service.

[vrf *vrf_name***] ip service source-ip {Loopback0 |** *interface_name***} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]**

[vrf *vrf_name***] no ip service source-ip {Loopback0 |** *interface_name***} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]**

Syntax Definitions

vrf_name	Name of the VRF.
Loopback0	Uses the Loopback0 interface as the source IP for the IP service.
interface_name	Specifies the name of the interface.
tftp	Configures the source IP address to be used by TFTP.
telnet	Configures the source IP address to be used by TELNET.
tacacs	Configures the source IP address to be used by TACACS.
swlog	Configures the source IP address to be used by SWLOG.
ssh	Configures the source IP address to be used by SSH.
snmp	Configures the source IP address to be used by SNMP.
sflow	Configures the source IP address to be used by sFlow.
radius	Configures the source IP address to be used by RADIUS.
ntp	Configures the source IP address to be used by NTP.
ldap	Configures the source IP address to be used by the LDAP server.
ftp	Configures the source IP address to be used by FTP.
dns	Configures the source IP address to be used by DNS.
all	Configures the source IP address to be used by all the applications.

Defaults

By default, the outgoing interface is taken as the source IP address for all the applications.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If for a particular application, specific source IP address is configured and the “all” option is also set, the configured source IP address for the application is used as the outgoing interface.
- Use the **no** form of this command to revert to the default behavior.
- This feature is supported on non-default VRF.

Examples

```
-> ip service source-ip loopback0 dns
-> ip service source-ip ipVlan100 ftp
```

Release History

Release 7.3.4; command introduced
Release 8.5R4; **ntp** option deprecated.
Release 8.6R2; **ntp** option re-introduced.

Related Commands

show ip service source-ip	Displays the IP service TCP/UDP port configuration and status.

MIB Objects

```
alaIpServiceSourceIPTable
   AlaIpServiceSourceIPAppIndex
   alaIpServiceSourceIPName
```

ip redist

Controls the conditions for redistributing IPv4 routes between different protocols.

[vrf *vrf_name***] ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} {all-routes | route-map** *route_map_name***} [admin-state {enable | disable}]**

no ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} [all-routes | route-map | *route_map_name***]**

Syntax Definitions

vrf_name	The name of an existing VRF instance.
local	Redistributes local routes.
static	Redistributes static routes.
rip	Specifies RIP as the source or destination (into) protocol.
ospf	Specifies OSPF as the source or destination (into) protocol.
isis	Specifies IS-IS as the source or destination (into) protocol.
bgp	Specifies BGP as the source or destination (into) protocol.
import	Redistributes imported routes to other routing protocols.
all-routes	Redistributes all routes. This option does not allocate route-map resources.
route_map_name	Name of an existing route map that controls the redistribution of routes between the source and destination protocol.
enable	Enables the administrative status of the redistribution configuration.
disable	Disables the administrative status of the redistribution configuration.

Defaults

If a VRF name is not specified with this command, routes are redistributed within the context of the active VRF instance.

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a route map redistribution configuration. If a route map name is not specified, all route maps associated with the redistribution configuration are removed.
- The source and destination protocols must be loaded and enabled before redistribution occurs.
- If the metric calculated for the redistributed route is greater than 15 (RIP_UNREACHABLE) or greater than the metric of an existing pure RIP route, the new route is not redistributed.

- Use the **ip route-map** commands described in this chapter to create a route map. Refer to the "Configuring IP" chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.

Examples

```
-> ip redist rip into bgp route-map rip-to-bgp1
-> ip redist rip into bgp route-map rip-to-bgp2
-> no ip redist rip into bgp route-map rip-to-bgp2
-> ip redist ospf into rip route-map ospf-to-rip
-> ip redist ospf into rip route-map ospf-to-rip disable
-> ip redist import into ospf route-map R1 status enable
```

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** and **import** parameters added.
Release 7.3.2; **all-routes** parameter added.

Related Commands

show ip redist	Displays the route map redistribution configuration.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip import	Configures a route map to import routes from GRT to the destination VRF.
show ip import	Displays the import route configuration details.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistSrcProtoId
   alaRouteMapRedistDestProtoId
   alaRouteMapRedistRouteMapIndex
   alaRouteMapRedistStatus
   alaRouteMapRedistAddressType
   alaRouteMapRedistRowStatus
```

ip access-list

Creates an access list for adding multiple IPv4 addresses to route maps.

ip access-list *access-list-name*

no ip access-list *access-list-name*

Syntax Definitions

access-list-name	Name of the access list (up to 20 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to delete the access list.

Examples

```
-> ip access-list access1
-> no ip access-list access1
```

Release History

Release 7.1.1; command introduced

Related Commands

ip access-list address	Adds IPv4 addresses to the specified IPv4 access list.
show ip access-list	Displays the details of the access list.

MIB Objects

```
alaRouteMapAccessListNameTable
   alaRouteMapAccessListName
   alaRouteMapAccessListNameIndex
   alaRouteMapAccessListNameAddressType
   alaRouteMapAccessListNameRowStatus
```

ip access-list address

Adds multiple IPv4 addresses to the specified IPv4 access list.

ip access-list *access-list-name* **address** *address/prefixLen* **[action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]**

no ip access-list *access-list-name* **address** *address/prefixLen*

Syntax Definitions

access-list-name	Name of the access list.
address/prefixLen	IP address/prefix length to be added to the access list.
permit	Permits the IP address.
deny	Denies the IP address.
all-subnets	Permits or denies all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Permits or denies only those routes that exactly match the IP address and the mask length.
aggregate	Permits an aggregate route if there are one or more routes that match or are subnets of this address.

Defaults

parameter	default
permit | deny	**permit**
all-subnets | no-subnets | aggregate	**all-subnets**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the address from the access list.
- The *access-list-name* must exist before you add multiple addresses to the list.
- The **action** parameters (**permit** and **deny**) determine if a route that matches the **redist-control** configuration for the IP address is allowed or denied.
- The **redist-control** parameters (**all-subnets, no-subnets**, and **aggregate**) defines the criteria used to determine if a route matches an address in the access list.
- Configuring the combination of **redist-control aggregate** with **action deny** is not allowed.
- Use this command multiple times with the same access list name to add multiple addresses to the existing access list.

Examples

```
-> ip access-list access1 address 10.0.0.0/8 action permit
-> ip access-list access1 address 11.1.0.0/16 action permit
-> ip access-list access1 address 10.1.1.0/24 redist-control aggregate
-> no ip access-list access1 address 10.0.0.0/8
```

Release History

Release 7.1.1; command introduced

Related Commands

ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
show ip access-list	Displays the contents of an IPv4 access list.

MIB Objects

```
alaRouteMapAccessListTable
   alaRouteMapAccessListIndex
   alaRouteMapAccessListAddress
   alaRouteMapAccessListAddressType
   alaRouteMapAccessListPrefixLength
   alaRouteMapAccessListAction
   alaRouteMapAccessListRedistControl
   alaRouteMapAccessListRowStatus
```

ip route-map action

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

ip route-map *route_map_name* **[sequence-number** ***number*****] action {permit | deny}**

no ip route-map *route_map_name* **[sequence-number** *number***]**

Syntax Definitions

route_map_name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
permit	Selects a route.
deny	Filters a route.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the entire route map by specifying only the *route_map_name*.
- Use the **no** form of this command to delete a specific sequence in the route map by specifying the **sequence-number**.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- Use this command to change the status of an existing route map to permit or deny.

Examples

```
-> ip route-map route1 sequence-number 10 action permit
-> no ip route-map route1
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapSequenceTable
   alaRouteMapSequenceIndex
   alaRouteMapSequenceNumber
   alaRouteMapSequenceAction
   alaRouteMapSequenceRowStatus
```

ip route-map match ip address

Matches the route with the specified IPv4 address or an address defined in the specified IPv4 access list.

ip route-map *route_map_name* **[sequence-number** ***number*****] match ip-address {***access-list-name* **|** ***ip_address/****prefixLen* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**

no ip route-map *route_map_name* **[sequence-number** ***number*****] match ip-address {***access-list-name* **|** *ip_address/prefixLen* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
access-list-name	The name of an IPv4 access list that contains IPv4 addresses to match.
ip_address/prefixLen	The destination IP address along with the prefix length of the routes to be selected.
all-subnets	Selects all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Selects only those routes that exactly match the IP address and the mask length.
aggregate	Creates an aggregate route if there are one or more routes that match the IP address.
permit	Permits a route based on the IP address or prefix constrained by redist-control.
deny	Denies a route based on the IP address or prefix constrained by redist-control.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match ip-address redist-control** parameter in the route map.
- Specify either the name of an existing IPv4 access list or an IPv4 address/prefix length with this command.
- Configuring the combination of **redist-control aggregate** with **deny** is not allowed.
- Multiple addresses in the same route map sequence are matched using the longest prefix match.

- If the best matching address is type **deny,** then the route is not selected. If the best matching address is type **permit** and the route map action is **deny,** the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name*, **sequence-number,** and *access-list-name* (if used) must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 3 match ip-address 10.1.1.1/8 redist-control no-subnets deny
-> no ip route-map 3 match ip-address 10.1.1.1 redist-control no-subnets deny
-> ip route-map route1 sequence-number 10 match ip-address list1
-> no ip route-map route1 sequence-number 10 match ip-address list1
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
ip access-list address	Adds IPv4 addresses to the specified IPv4 access list.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ipv6 address

Matches the route with the specified IPv6 address or an address defined in the specified IPv6 access list.

ip route-map *route_map_name* **[sequence-number** *number***] match ipv6-address {***access-list-name* **|** *ipv6_address/prefixLen* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**

no ip route-map *route_map_name* **[sequence-number** *number***] match ipv6-address** *ipv6_address/prefixLen* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**

Syntax Definitions

route_map_name	The name of the route map (up to 20 characters).
number	A number that links together the route maps. The range is 1–100.
access-list-name	The name of an IPv6 access list that contains IPv6 addresses to match.
ipv6_address/prefixLen	The destination IPv6 address along with the prefix length of the routes to be selected.
all-subnets	Selects all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Selects only those routes that exactly match the IP address and the mask length.
aggregate	Creates an aggregate route if there are one or more routes that match the IPv6 address.
permit	Permits a route based on the IPv6 address or prefix constrained by redist-control.
deny	Denies a route based on the IPv6 address or prefix constrained by redist-control.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv6-address redist-control** parameter in the route map.
- Specify either the name of an existing IPv6 access list or an IPv6 address/prefix length with this command.
- Configuring the combination of **redist-control aggregate** with **deny** is not allowed.
- Multiple addresses in the same route map sequence are matched using the longest prefix match.

- If the best matching address is type **deny,** then the route is not selected. If the best matching address is type **permit** and the route map action is **deny,** the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 3 match ipv6-address 2001::1/64 redist-control no-subnets deny
-> no ip route-map 3 match ipv6-address 2001::1/64 redist-control no-subnets deny
-> ip route-map route1 sequence-number 10 match ipv6-address list1
-> no ip route-map route1 sequence-number 10 match ipv6-address list1
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ipv6 access-list	Creates an access list for adding multiple IPv6 addresses to route maps.
ipv6 access-list address	Adds IPv6 addresses to the specified IPv6 access list.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ip-nexthop

Matches any routes that have a next-hop router address permitted by the specified access list name or the IP address specified in the route map.

ip route-map *route_map_name* **[sequence-number** *number***] match ip-nexthop {***access-list-name* | *ip_address/prefixLen* **[permit | deny]}**

no ip route-map *route_map_name* **[sequence-number** *number***] match ip-nexthop {***access-list-name* | *ip_address/prefixLen* **[permit | deny]}**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
access-list-name	The access list that matches the route nexthop IP address.
ip_address/prefixLen	The IP address along with the prefix length that matches any nexthop IP address within the specified subnet.
permit	Permits a route based on the IP nexthop.
deny	Denies a route based on the IP nexthop.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match ip-nexthop** parameter in the route map.
- If the best matching nexthop is type **deny,** then the route is not selected. If the best matching nexthop is type **permit** and the route map action is **deny,** the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name*, **sequence-number,** and *access-list-name* must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match ip-nexthop list1
-> no ip route-map route1 sequence-number 10 match ip-nexthop list1
-> ip route-map route1 sequence-number 10 match ip-nexthop 10.0.0.0/8
-> no ip route-map route1 sequence-number 10 match ip-nexthop 10.0.0.0/8
```

Release History

Release 7.1.1; command introduced

Related Commands

ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ipv6-nexthop

Matches any routes that have an IPv6 next-hop router address permitted by the specified access list name or the IPv6 address specified in the route map.

ip route-map *route_map_name* **[sequence-number** *number***] match ipv6-nexthop {***access-list-name* **|** *ipv6_address/prefixLen* **[permit | deny]}**

no ip route-map *route_map_name* **[sequence-number** *number***] match ipv6-nexthop {***access-list-name* **|** *ipv6_address/prefixLen* **[permit | deny]}**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
access-list-name	The access list that matches the route nexthop IPv6 address.
IPv6_*address/prefixLen*	The IPv6 address along with the prefix length that matches any nexthop IP address within the specified subnet.
permit	Permits a route based on the IPv6 nexthop.
deny	Denies a route based on the IPv6 nexthop.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv6-nexthop** parameter in the route map.
- If the best matching nexthop is type **deny,** then the route is not selected. If the best matching nexthop is type **permit** but the route map action is **deny,** the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name*, **sequence-number,** and *access-list-name* must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match ipv6-nexthop list1
-> no ip route-map route1 sequence-number 10 match ipv6-nexthop list1
-> ip route-map route1 sequence-number 10 match ipv6-nexthop 2001::/64
-> no ip route-map route1 sequence-number 10 match ipv6-nexthop 2001::/64
```

Release History

Release 7.1.1; command introduced

Related Commands

ipv6 access-list	Creates an access list for adding multiple IPv6 addresses to route maps.
ipv6 access-list address	Adds IPv6 addresses to the specified IPv6 access list.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match tag

Matches the tag value specified in the route map with the one on which the routing protocol learned the route.

ip route-map *route_map_name* **[sequence-number** *number***] match tag** *tag-number*

no ip route-map *route_map_name* **[sequence-number** *number***] match tag** *tag_number*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
tag_number	The tag number.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match tag** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match tag 4
-> no ip route-map route1 sequence-number 10 match tag 4
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ipv4-interface

Matches the IPv4 interface name specified in the route map with the one that the routing protocol learned the route on.

ip route-map *route_map_name* **[sequence-number** *number***] match ipv4-interface** *interface_name*

no ip route-map *route_map_name* **[sequence-number** *number***] match ipv4-interface** *interface_name*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
interface_name	Specifies the interface name of the outgoing interface of the route.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv4-interface** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match ipv4-interface int4
-> no ip route-map route1 sequence-number 10 match ipv4-interface int4
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match ipv6-interface

Matches the IPv6 interface name specified in the route map with the one that the routing protocol learned the route on.

ip route-map *route_map_name* **[sequence-number** *number***] match ipv6-interface** *interface_name*

no ip route-map *route_map_name* **[sequence-number** *number***] match ipv6-interface** *interface_name*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
interface_name	Specifies the interface name of the outgoing interface of the route.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv6-interface** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match ipv6-interface int6
-> no ip route-map route1 sequence-number 10 match ipv6-interface int6
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match metric

Matches the metric value specified in the route map with the actual metric value of the route.

ip route-map *route_map_name* **[sequence-number** *number***] match metric** *metric* **[deviation** *deviation***]**

no ip route-map *route_map_name* **[sequence-number** *number***] match metric** *metric* **[deviation** *deviation***]**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
metric	The metric value that matches a specified metric.
deviation	The deviation value. If deviation is included, the route metric can have any value within the range (metric-deviation to metric+deviation).

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match metric** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match metric 4
-> no ip route-map route1 sequence-number 10 match metric 4
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match route-type

Matches the specified route type with actual route type of the route.

ip route-map *route_map_name* **[sequence-number** *number***] match route-type {internal | external [type1 | type2] | level1 | level2}**

no ip route-map *route_map_name* **[sequence-number** *number***] match route-type {internal | external [type1 | type2] | level1 | level2}**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
internal	Matches OSPF/BGP internal routes.
external	Matches OSPF/BGP external routes.
type1	Matches OSPF external Type-1 routes, which gives the full metric calculation for the complete path including internal as well as external cost.
type2	Matches OSPF external Type-2 routes, which gives the external redistribution metric only to the ASBR.
level1	Matches IS-IS Level-1 routes only.
level2	Matches IS-IS Level-2 routes only.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match route-type** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 match route-type internal
-> no ip route-map 111 sequence-number 50 match route-type internal
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match protocol

Matches the protocol specified in the route map with the protocol of the route.

ip route-map *route_map_name* **[sequence-number** *number***] match protocol {local | static | rip | ospf | isis | bgp}**

no ip route-map *route_map_name* **[sequence-number** *number***] match protocol {local | static | rip | ospf | isis | bgp}**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
local	Matches a local interface route.
static	Matches a static route.
rip	Matches a RIP route.
ospf	Matches an OSPF route.
isis	Matches an IS-IS route.
bgp	Matches a BGP route.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match protocol** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match protocol local
-> no ip route-map route1 sequence-number 10 match protocol local
```

Release History

Release 7.3.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map match name

Matches the name of a static route specified in the route map with the name of the static route.

ip route-map *route_map_name* **[sequence-number** *number***] match name** *string*

no ip route-map *route_map_name* **[sequence-number** *number***] match name** *string*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
name *string*	The name of the static route to match.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **match name** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map route1 sequence-number 10 match name Route-Bldg1
-> no ip route-map route1 sequence-number 10 match name Route-Bldg1
```

Release History

Release 7.3.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set metric

Configures the metric value of the route being distributed.

ip route-map *route_map_name* **[sequence-number** *number***] set metric** *metric* **[effect {add | subtract | replace | none}]**

no ip route-map *route_map_name* **[sequence-number** *number***] set metric** *metric* **[effect {add | subtract | replace | none}]**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
metric	Configures the metric value of the route. A value of 0 is not allowed.
add	Adds the configured metric value to the actual metric value.
subtract	Subtracts the configured metric value from the actual metric value.
replace	Replaces the actual metric value with the configured metric value.
none	Uses the actual metric value of the route. The configured metric value is ignored. Use any value except 0.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **set metric** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set metric 30 effect add
-> no ip route-map 111 sequence-number 50 set metric 30 effect add
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set metric-type

Configures the metric type for the redistributed route.

ip route-map *route_map_name* **[sequence-number** *number***] set metric-type {internal | external [type1 | type2]}**

no ip route-map *route_map_name* **[sequence-number** *number***] set metric-type {internal | external [type1 | type2]}**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
internal	Sets the metric type to internal for routes redistributed into BGP.
external	Sets the metric type to external for routes redistributed into BGP.
type1	Sets the metric type to external type1 for routes redistributed into OSPF, which gives the full metric calculation for the complete path including internal as well as external cost.
type2	Sets the metric type to external type2 for routes redistributed into OSPF, which gives the external redistribution metric only to the ASBR.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **set metric-type** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set metric-type internal
-> no ip route-map 111 sequence-number 50 set metric-type internal
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set tag

Configures the tag value of the selected routes.

ip route-map *route_map_name* **[sequence-number** *number***] set tag** *tag_number*

no ip route-map *route_map_name* **[sequence-number** *number***] set tag** *tag_number*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
tag_number	Configures the tag number.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **set tag** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set tag 23
-> no ip route-map 111 sequence-number 50 set tag 23
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set community

Configures the community name of the route being redistributed into BGP.

ip route-map *route_map_name* **[sequence-number** *number***] set community** *community_string*

no ip route-map *route_map_name* **[sequence-number** *number***] set community** *community_string*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
community_string	Defines a community for an aggregate route. Community names range from 0 to 70 characters.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **set community** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set community 29
-> no ip route-map 111 sequence-number 50 set community 29
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set local-preference

Configures the local preference value for a route being distributed into BGP.

ip route-map *route_map_name* **[sequence-number** *number***] set local-preference** *value*

no ip route-map *route_map_name* **[sequence-number** *number***] set local-preference** *value*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
value	Configures the local-preference value for routes being redistributed in to BGP. The value is between 0 and 4294967295.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **set local-preference** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **set** criteria.
- The local preference attribute is used to set preference to an exit point from the local autonomous system (AS).
- If there are multiple exit points from the AS, the local preference attribute is used to select the exit point for a specific route.

Examples

```
-> ip route-map 111 sequence-number 50 set local-preference 4
-> no ip route-map 111 sequence-number 50 set local-preference 4
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set level

Configures the level of the selected ISIS route.

ip route-map *route_map_name* **[sequence-number** *number***] set level {level1 | level2 | level1-2}**

no ip route-map *route_map_name* **[sequence-number** *number***] set level {level1 | level2 | level1-2}**

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
level1	Matches IS-IS Level-1 routes only.
level2	Matches IS-IS Level-2 routes only.
level1-2	Matches IS-IS Level1-2 routes**.**

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **set level** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set level level1
-> no ip route-map 111 sequence-number 50 set level level1
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set ip-nexthop

Configures the IP address of the next hop in a route map.

ip route-map *route_map_name* **[sequence-number** *number***] set ip-nexthop** *ip_address*

no ip route-map *route_map_name* **[sequence-number** *number***] set ip-nexthop** *ip_address*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
ip_address	IP address of the next hop.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **set ip-nexthop** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 222 sequence-number 50 set ip-nexthop 128.251.17.224
-> no ip route-map 222 sequence-number 50 set ip-nexthop 128.251.17.224
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIPRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

ip route-map set ipv6-nexthop

Configures the IPv6 address of the next hop in a route map.

ip route-map *route_map_name* **[sequence-number** *number***] set ipv6-nexthop** *ipv6_address*

no ip route-map *route_map_name* **[sequence-number** *number***] set ipv6-nexthop** *ipv6_address*

Syntax Definitions

route_map_name	The name of the route map.
number	A number that links together the route maps. The range is 1–100.
ipv6_address	IPv6 address of the next hop.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the **set ipv6-nexthop** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route_map_name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 222 sequence-number 50 set ipv6-nexthop 2001::1
-> no ip route-map 222 sequence-number 50 set ipv6-nexthop 2001::1
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIPRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

vrf

Configures and selects a virtual routing and forwarding (VRF) instance on the switch.

vrf [create] [*vrf_name* | **default] [profile {max | low}]**

no vrf *vrf_name*

Syntax Definitions

create	Creates a new VRF instance with the specified VRF name.
vrf_name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
default	Optional. Selects the default VRF instance.
max	Creates a VRF with the maximum profile capabilities.
low	Creates a VRF with the minimum (lowest) capabilities. Low profile VRFs use less system resources.

Defaults

A default VRF instance exists in the switch configuration. All applications that are not VRF aware belong to this instance.

Parameter	Default
vrf_name | **default**	default VRF instance
max | low	max profile

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- To create a new VRF instance, use the **create** parameter with this command. For example, **vrf create IpOne** creates a new “IpOne” VRF instance. When a new instance is created, that instance automatically becomes the current CLI context.
- If the **create** keyword is not specified, then this command will select the specified VRF name as the current CLI context. If the VRF instance does not exist, an error message is displayed.
- Use the **no** form of this command to delete a VRF instance. Deleting the default instance is not allowed. In addition, any interfaces configured for a VRF instance are automatically removed when the instance is deleted.
- To return to the default VRF instance from within the context of another instance, enter the **vrf** command with or without the optional **default** parameter (for example, **vrf** or **vrf default**).
- Configuring a VRF instance name is case sensitive. Use the **show vrf** command to verify the VRF instance configuration before selecting, adding, or removing instances.
- If the name of an existing instance is specified with this command, VRF changes the command prompt to reflect the specified instance name. All CLI commands entered at this point are applied within the context of the active VRF instance.

- It is also possible to configure other instances from within the CLI context of the default VRF instance by entering the **vrf** command followed by the instance name. For example, entering **vrf IpOne ip interface intf100 address 100.1.1.1/24 vlan 100** is applied to the IpOne instance even though IpOne is not the active CLI context.
- The type of profile assigned to a VRF instance determines the routing protocols and capabilities supported within that instance. For example:
  - Low profile VRFs only support IPv4 and VRRP with routing capabilities restricted to static and imported routes. In addition, limiting low profiles to 9 routes and 3 IP interfaces is highly recommended.
  - IPv6 routing protocols (such as BGP, IS-IS, PIM, RIPng, OSPFv3, and VRRPv3) are only supported on max profile VRFs.
- Profiles are not configurable for the default VRF, which provides full routing capabilities.
- Changing the profile for an existing VRF instance is not allowed. To change the profile, first delete the VRF then create it again with a different profile.

Examples

The following command examples create new VRF instances:

```
-> vrf create IpOne
IpOne:: ->

IpOne:: -> vrf create IpTwo
IpTwo:: ->

-> vrf create IpThree profile low
IpThree::->
```

The following command examples select a VRF instance to change the CLI context:

```
-> vrf IpTwo
IpTwo:: ->

-> vrf IpFour
ERROR: VRF IpFour does not exist.
```

The following command examples return the CLI context to the default VRF instance:

```
IpTwo:: -> vrf
->

IpTwo:: -> vrf default
->
```

The following command example configures an IP interface for the “IpOne” VRF instance from within the context of the default VRF instance:

```
-> vrf IpOne ip interface intf100 address 100.1.1.1/24 vlan 100
->
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; **max** and **low** parameters added to define VRF profiles.
Release 8.4.1.R03; **create** parameter added.

Related Commands

show vrf	Displays the VRF instance configuration for the switch.
show vrf-profiles	Displays the VRF profile resources for the switch.
ip export	Exports VRF routes to the Global Routing Table (GRT).
ip import	Imports VRF routes from the GRT.

MIB Objects

```
alaVirutalRouterNameTable
   alaVirtualRouterName
   alaVirtualRouterNameIndex
   alaVirtualRouterNameRowStatus
   alaVirtualRouterProfile
```

ip export

Exports routes from the source VRF to the Global Routing Table (GRT) or to all VRF instances. All routes are exported or a route map can be specified to filter exported routes

[vrf *vrf_name***] ip export {all-routes | route-map** *route_map_name* | **to-all-vrfs {all-routes | route-map** *route_map_name***}}**

[vrf *vrf_name***] no ip export**

Syntax Definitions

vrf_name	The name of an existing VRF instance. Routes are exported from this source VRF to the GRT.
all-routes	Exports all routes from the source VRF to the GRT. This option does not allocate route-map resources.
route_map_name	The name of an existing route-map to use for filtering routes that are exported from the source VRF to the GRT.
to-all-vrfs all-routes	Exports all routes to all of the other VRF instances, except to VRFs that already have an import configured for the source (export) VRF.
to-all-vrfs route-map *route_map_name*	The name of an existing route map to use for filtering routes that are exported from the source VRF to all other VRF instances.

Defaults

- If a source VRF name is not specified with this command, routes are exported from within the context of the active VRF instance to the GRT.
- If there are no VRF instances configured on the switch, the routes are exported from the default VRF to the GRT.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable exporting of routes from the VRF to GRT.
- The route map name specified with this command must already exist in the switch configuration. See the **ip route-map** commands in this guide and the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.
- A route map created to filter exported VRF routes can contain any of the following match and set options:
  - Match options: ip-address, ip-next-hop, tag, protocol, ipv4-interface, metric, route-type, name
  - Set options: tag, metric
- A route map with redist control of aggregate is supported when exporting IP routes, but it is not supported when importing IP routes.
- Only one route map per source VRF or ISID is allowed for filtering exported routes.

- Only those FDB (Forwarding Routing Database) routes that match the conditions of the route map are exported to GRT.
- Modifying a route map that is assigned to a VRF or ISID through the **ip import** or **ip export** command is supported.

Examples

The following commands export routes from the current VRF routing table (or from the default VRF if there are no other VRFs configured) to the GRT:

```
-> ip export route-map R1
-> ip export all-routes
-> ip export to-all-vrfs all-routes
-> ip export to-all-vrfs route-map R2
-> no ip export
```

The following commands export routes from the “vrf2” routing table to the GRT even though the command line is operating within the context of the default VRF instance:

```
-> vrf vrf2 ip export route-map R1
-> vrf vrf2 ip export all-routes
-> vrf vrf2 ip export to-all-vrfs all-routes
-> vrf vrf2 ip export to-all-vrfs route-map R2
-> no vrf vrf2 ip export
```

The following commands first change the command line context to the “vrf1” instance so that all subsequent commands export routes from “vrf1” without having to specify the VRF name with each command:

```
-> vrf vrf1
vrf1::-> ip export route-map R1
vrf1::-> ip export all-routes
vrf1::-> ip export to-all-vrfs all-routes
vrf1::-> ip export to-all-vrfs route-map R2
vrf1::-> no ip export
```

Release History

Release 7.3.1; command introduced.
Release 7.3.2; **all-routes** and **to-all-vrfs** parameters added.

Related Commands

vrf	Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match protocol	Matches the protocol specified in the route map with the protocol of the route.
show ip export	Displays the export route configuration details.
show ip global-route-table	Displays the GRT for all the routes that are exported from the VRFs.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIprmExportRouteMap
alaIprmExportToAllVrfsRouteMap
```

ip import

Imports VRF or Shortest Path Bridging (SPB) service instance identifier (ISID) routes from the GRT to the destination VRF. All routes are imported or a route map can be specified to filter imported routes.

[vrf *dest_vrf_name***] ip import {vrf {***src_vrf_name* **| default} | isid** *instance_id***} {all-routes | route-map** *route_map_name***}**

[vrf *dest_vrf_name***] no ip import {vrf {***src_vrf_name* **| default} | isid** *instance_id***}**

Syntax Definitions

dest_vrf_name	The name of the destination VRF instance into which routes are imported from the GRT.
src_vrf_name	The name of the source VRF instance from which routes were exported to the GRT. Routes from this instance are imported from the GRT into the specified destination VRF instance.
default	Default VRF. The routes are imported from the default VRF instance.
instance_id	An existing ISID number that identifies an SPB service in a provider backbone bridge (PBB) network. The routes for this ISID number are imported from the GRT into the current or specified VRF instance.
all-routes	Imports all routes from the source VRF instance. Imported routes are not filtered.
route_map_name	The name of an existing route map to use for filtering routes that are imported from the GRT to the destination VRF. Imported routes are filtered based on the options defined in the route map.

Defaults

If a destination VRF name is not specified with this command, routes are imported from the GRT into the context of the active VRF instance.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the IP import routes configuration for the specified VRF instance or ISID.
- The route map name specified with this command must already exist in the switch configuration. See the **ip route-map** commands in this guide and the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.
- A route map created to filter imported VRF or ISID routes can contain any of the following match and set parameter options:
  - Match options: ip-address, ip-next-hop, tag, metric
  - Set options: tag, metric

- A route map with redist control of aggregate is supported when exporting IP routes, but it is not supported when importing IP routes.
- Only one route map per source (imported) VRF or ISID is allowed.
- Modifying a route map that is assigned to a VRF or ISID through the **ip import** or **ip export** command is supported.
- Leaked routes are only for forwarding. If a local route is leaked, that interface is not accessible in the importing VRF. Another switch will not be able to ping the interface in the import VRF.

Examples

```
-> ip import vrf V1 route-map R2
-> ip import vrf V2 all-routes
-> ip import isid 1500 route-map R1
-> ip import isid 2000 all-routes
-> no ip import vrf V1
-> no ip import isid 1500
```

Release History

Release 7.3.1; command introduced.
Release 7.3.2; **isid** and **all-routes** parameters added.

Related Commands

vrf	Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match protocol	Matches the protocol specified in the route map with the protocol of the route.
show ip import	Displays the import route configuration details.
show ip global-route-table	Displays the GRT for all the routes that are exported from the VRFs.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIprmImportVrfTable
   alaIprmImportVrfName
   alaIprmImportVrfRouteMap
   alaIprmImportVrfRowStatus
alaIprmImportIsidTable
   alaIprmImportIsid
   alaIprmImportIsidRouteMap
   alaIprmImportIsidRowStatus
```

show ip export

Displays the export route configuration details.

[vrf *vrf_name***] show ip export**

Syntax Definitions

vrf_name	The name of an existing VRF instance.

Defaults

By default, the export route configuration for the active VRF instance is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If a VRF is specified, the export route configuration for that VRF is displayed.

Examples

```
-> show ip export
Export Route Map: leak-out

-> vrf vrf1 show ip export
Export Route Map: none (all-routes)

vrf2::-> show ip export
Export Route Map: none (all-routes) -> To All VRFs
```

Release History

Release 7.3.1; command introduced.

Related Commands

ip export	Exports routes from the source VRF to the Global Routing Table (GRT) or to all VRF instances.

MIB Objects

```
alaIprmExportRouteMap
alaIprmExportToAllVrfsRouteMap
```

show ip import

Displays the import route configuration details.

[vrf *vrf_name***] show ip import**

Syntax Definitions

vrf_name	The name of an existing VRF instance.

Defaults

By default, the import route configuration for the active VRF instance is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If a VRF is specified, the import route configuration for that VRF is displayed.

Examples

```
-> show ip import
Type  Source               RouteMap
-----+--------------------+----------------------
vrf    Customer1           leak-in
vrf    Customer2           none (all-routes)
isid   1000                isid1000-filter
```

output definitions

Type	The type of imported route (**vrf** or **isid**).
Source	The name of the VRF instance or the Shortest Path Bridging service instance identifier (ISID) from which routes are imported to the VRF.
RouteMap	The name of the route map filter or **none (all-routes)**.

Release History

Release 7.3.1; command introduced.
Release 7.3.2; **VRF Name** and **Description** fields renamed **Type** and **Source,** imported ISID route entries added to the table.

Related Commands

ip import	Imports VRF or Shortest Path Bridging ISID routes from the GRT to the destination VRF.

MIB Objects

```
alaIprmImportVrfTable
   alaIprmImportVrfName
   alaIprmImportVrfRouteMap
   alaIprmImportVrfRowStatus
alaIprmImportIsidTable
   alaIprmImportIsid
   alaIprmImportIsidRouteMap
   alaIprmImportIsidRowStatus
```

show ip global-route-table

Displays the contents of the Global Routing Table (GRT) for all the routes that are exported from VRF instances or from Shortest Path Bridging service instance identifiers (ISIDs). This command is only available within the context of the default VRF instance.

show ip global-route-table [export-vrf *vrf_name***]**

Syntax Definitions

vrf_name	The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

By default, exported routes are displayed for all VRF instances and ISIDs.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **export-vrf** parameter to display exported routes for a specific VRF instance.

Examples

```
-> show ip global-route-table
Type  Source               Destination        Gateway         Metric     Tag
-----+--------------------+------------------+---------------+----------+----------
 vrf   Customer1            10.0.0.0/8         12.1.1.2        1          100
 vrf   Customer2            11.0.0.0/8         12.1.1.3        2          0
isid   1000                 12.0.0.0/8         12.1.1.4        1          2
```

output definitions

Type	The type of exported route (**vrf** or **isid**).
Source	The name of the VRF instance or the Shortest Path Bridging service instance identifier (ISID) from which routes are exported to the GRT.
Destination	The address of the route.
Gateway	The next hop for the destination address.
Metric	The metric of the exported route.
Tag	The tag of the exported route.

Release History

Release 7.3.1; command introduced.
Release 7.3.2; **VRF Name** and **Description** fields renamed **Type** and **Source,** exported ISID route entries added to the table.

Related Commands

ip export	Configures a route map to export routes from the source VRF to Global Routing Table (GRT).
show ip export	Displays the export route configuration details.

MIB Objects

```
alaGrtRouteTable
   alaGrtRouteDistinguisher
   alaGrtRouteDest
   alaGrtRouteMaskLen
   alaGrtRouteNextHop
   alaGrtRouteMetric
   alaGrtRouteTag
   alaGrtRouteVrfName
   alaGrtRouteIsid
```

arp

Adds a permanent entry to the ARP table. To forward packets, the switch dynamically builds an ARP Table to match the IP address of a device with its physical (MAC) address. These entries age out of the table when the timeout value is exceeded. This command is used to add a permanent entry to the table. Permanent entries do not age out of the table.

arp *ip_address mac_address* **[alias] [arp-name** *name***] [interface** *interface_name***] [port** *chassis/slot/port***] [linkagg** *agg_id***]**

no arp *ip_address* **[alias]**

Syntax Definitions

ip_address	IP address of the device you are adding to the ARP table.
mac_address	MAC address of the device in hexadecimal format (for example, 00.00.39.59.f1.0c).
alias	Specifies that the switch will act as an alias (or proxy) for this IP address. When the alias option is used, the switch responds to all ARP requests for the specified IP address with its own MAC address. *This parameter is not supported on the OmniSwitch 9900.* The proxy feature can also be enabled for an IP interface using the **ip interface** command. When enabled, ARP requests return the MAC address of the IP router interface and all traffic within the VLAN is routed.
name	The name to assign to this ARP entry.
interface_name	Name of the interface to be used for ARP resolution.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
agg_id	The link aggregate ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a permanent ARP entry.
- Configuring a permanent ARP entry with a multicast address is also supported. This is done by specifying a multicast address for the *ip_address* parameter instead of a unicast address.
- Using the **arp alias** command is not related to proxy ARP as defined in RFC 925. Instead, **arp alias** is similar to the Local Proxy ARP feature, except that it is used to configure the switch as a proxy for only *one* IP address.

- As most hosts support the use of address resolution protocols to determine cache address information (called dynamic address resolution), it is not required to specify permanent ARP cache entries.
- Only the IP address is required when deleting an ARP entry from the table.

Examples

```
-> arp 171.11.1.1 00:05:02:c0:7f:11
-> arp 171.11.1.1 00:05:02:c0:7f:11 interface int1
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **interface** parameter added.

Related Commands

ip distributed-arp admin-state	Deletes all dynamic entries from the ARP table.
ip interface	Enables or disables the Local Proxy ARP feature for an IP interface. When enabled, all traffic within the VLAN is routed. ARP requests return the MAC address of the IP router interface.
show arp	Displays the ARP table.

MIB Objects

```
ipNetToMediaTable
   ipNetToMediaIfIndex
   ipNetToMediaNetAddress
   ipNetToMediaPhyAddress
   ipNetToMediaType
alaIpNetToMediaTable
   alaIpNetToMediaPhyAddress
   alaIpNetToMediaProxy
```

ip distributed-arp admin-state

Enables or disables the distributed ARP feature.

ip distributed-arp admin-state {enable | disable}

Syntax Definitions

enable	Dynamically assigns a Network Interface (NI) as the designated-NI for all the ARP entries on an IP interface.
disable	Disables the distributed ARP feature.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

Not supported in this release.

Usage Guidelines

- Use this feature to dynamically assign a Network Interface (NI) as the designated-NI for all the ARP entries. The NI with maximum number of active ports for that IP subnet is assigned.
- To reset or update the dynamically assigned NI, the feature must be disabled and then enabled.

Examples

```
-> ip distributed-arp admin-state enable
-> ip distributed-arp admin-state disable
```

Release History

Release 7.3.4; command introduced;
Release 8.6R2; command deprecated.

Related Commands

show ip arp utilization	Displays the designated NIs for the interfaces and the NI utilization.
show ip interface	Displays the configuration and status of IP interfaces.

MIB Objects

```
alaIpDistributedArp
```

clear arp-cache

Deletes all dynamic entries from the ARP table.

clear arp-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only clears dynamic entries. If permanent entries have been added to the table, they must be removed using the **no** form of the **ip service** command.
- Dynamic entries remain in the ARP table until they time out. The switch uses the MAC Address table timeout value as the ARP timeout value. Use the **mac-learning aging-time** command to set the timeout value.

Examples

```
-> clear arp-cache
```

Release History

Release 7.1.1; command introduced

Related Commands

ip service	Adds a permanent entry to the ARP table.
show arp	Displays the ARP table.

MIB Objects

```
alaIpClearArpCache
```

ip dos arp-poison restricted-address

Adds or deletes an ARP Poison restricted address.

ip dos arp-poison restricted-address *ip_address*

no ip dos arp-poison restricted-address *ip_address*

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove an already configured ARP Poison restricted address.

Examples

```
-> ip dos arp-poison restricted-address 192.168.1.1
-> no ip dos arp-poison restricted-address 192.168.1.1
```

Release History

Release 7.1.1; command introduced

Related Commands

ip service	Adds a permanent entry to the ARP table.
show arp	Displays the ARP table.

MIB Objects

```
alaDoSArpPoisonTable
   alaDoSArpPoisonIpAddr
   alaDosArpPoisonRowStatus
```

arp filter

Configures an ARP filter that determines if ARP Request packets containing a specific IP address are processed by the switch or discarded.

arp filter *ip_address* **[mask** *ip_mask***] [***vlan_id***] [sender | target] [allow | block]**

no arp filter *ip_address*

Syntax Definitions

ip_address	The IP address to use for filtering ARP packet IP addresses.
ip_mask	An IP mask that identifies which part of the ARP packet IP address is examined for filtering (for example, mask 255.0.0.0 filters on the first octet of the ARP packet IP address).
vlan_id	A VLAN ID that specifies that only ARP packets for a specific VLAN are filtered.
sender	The sender IP address in the ARP packet is used for ARP filtering.
target	The target IP address in the ARP packet is used for ARP filtering.
allow	ARP packets that meet filter criteria are processed.
block	ARP packets that meet filter criteria are discarded.

Defaults

parameter	default
vlan_id	0 (no VLAN)
ip_mask	255.255.255.255
sender | target	**target**
allow | block	**block**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete an ARP filter.
- If there are no filters configured for the switch, all ARP Request packets received are processed.
- Up to 200 filters are allowed on each switch.
- If sender or target IP address in an ARP Request packet does not match any filter criteria, the packet is processed by the switch.
- ARP filtering is used in conjunction with the Local Proxy ARP application; however, ARP filtering is available for use on its own and/or with other applications.

Examples

```
-> arp filter 171.11.1.1
-> arp filter 172.0.0.0 mask 255.0.0.0
-> arp filter 198.0.0.0 mask 255.0.0.0 sender
-> arp filter 198.172.16.1 vlan 200 allow
-> no arp filter 171.11.1.1
```

Release History

Release 7.1.1; command introduced

Related Commands

clear arp filter	Clears all ARP filters from the filter database.
ip interface	Enables or disables the Local Proxy ARP feature on an IP interface. When enabled, all traffic within the VLAN is routed. ARP requests return the MAC address of the IP router interface.
show ip arp utilization	Displays the ARP filter configuration.

MIB Objects

```
alaIpArpFilterTable
   alaIpArpFilterIpAddr
   alaIpArpFilterIpMask
   alaIpArpFilterVlan
   alaIpArpFilterMode
   alaIpArpFilterType
```

clear arp filter

Clears the ARP filter database of all entries.

clear arp-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command clears all ARP filters configured on the switch. To remove an individual filter entry, use the **no** form of the **arp filter** command.

Examples

```
-> clear arp filter
```

Release History

Release 7.1.1; command introduced

Related Commands

arp filter	Configures an ARP filter to allow or block the processing of specified ARP Request packets.
show ip arp utilization	Displays the ARP filter configuration.

MIB Objects

```
alaIpClearArpFilter
```

icmp type

Enables or disables a specific type of ICMP message, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp type *type* **code** *code* **{{enable | disable} | min-pkt-gap** *gap***}**

Syntax Definitions

type	The ICMP packet type. This is conjunction with the ICMP code that determines the type of ICMP message being specified.
code	The ICMP code type. This is conjunction with the ICMP type that determines the type of ICMP message being specified.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | **disable**	disabled
gap	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows the user to enable or disable all types of ICMP messages, and set the minimum packet gap between messages of the specified type.
- Enabling **Host unreachable** and **Network unreachable** messages are not recommended as it can cause the switch instability due to high-CPU conditions depending upon the volume of traffic required by these messages.
- While this command can be used to enable or disable all ICMP message, some of the more common ICMP messages have their own CLI commands, as described in the pages below. The following ICMP messages have specific commands to enable and disable:

ICMP Message	Command
Network unreachable (type 0, code 3)	**icmp unreachable**
Host unreachable (type 3, code 1)	**icmp unreachable**
Protocol unreachable (type 3, code 2)	**icmp unreachable**
Port unreachable (type 3, code 3)	**icmp unreachable**
Echo reply (type 0, code 0)	**icmp echo**
Echo request (type 8, code 0)	**icmp echo**
Timestamp request (type 13, code 0)	**icmp timestamp**
Timestamp reply (type 14, code 0)	**icmp timestamp**
Address Mask request (type 17, code 0)	**icmp addr-mask**
Address Mask reply (type 18, code 0)	**icmp addr-mask**

Examples

```
-> icmp type 4 code 0 enabled
-> icmp type 4 code 0 min-pkt-gap 40
-> icmp type 4 code 0 disable
```

Release History

Release 7.1.1; command introduced

Related Commands

icmp messages	Enables or disables all ICMP messages.
show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp unreachable

Enables or disables ICMP messages pertaining to unreachable destinations, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp unreachable [net-unreachable | host-unreachable | protocol-unreachable | port-unreachable] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

net-unreachable	Sets the unreachable network ICMP message.
host-unreachable	Sets the unreachable host ICMP message.
protocol-unreachable	Sets the unreachable protocol ICMP message.
port-unreachable	Sets the unreachable port ICMP message.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	enable
gap	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command enables ICMP messages relating to unreachable destinations. Unreachable networks, hosts, protocols, and ports can all be specified.
- Enabling **host-unreachable** and **net-unreachable** messages are not recommended as it can cause the switch instability due to high-CPU conditions depending upon the volume of traffic required by these messages.
- The unreachable ICMP messages can also be enabled, disabled, and modified using the **icmp type** command. See the **icmp type** command information on the type and code for the unreachable ICMP messages.

Examples

```
-> icmp unreachable net-unreachable enable
-> icmp unreachable host-unreachable enable
-> icmp unreachable protocol-unreachable enable
-> icmp unreachable port-unreachable enable
```

```
-> icmp unreachable port-unreachable min-pkt-gap 50
```

Release History

Release 7.1.1; command introduced

Related Commands

show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp echo

Enables or disables ICMP echo messages, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp echo [request | reply] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

request	Specifies the echo request ICMP message.
reply	Specifies the echo reply ICMP message.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**enable**
gap	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command sets the ICMP echo messages. An echo request is sent to a destination, and must be responded to with an echo reply message that contains the original echo request.
- Using this command without specifying a request or reply enables, disables, or sets the minimum packet gap for both types.
- The echo ICMP messages can also be enabled, disabled, and modified using the **icmp type** command. See the **icmp type** command information on the type and code for the echo ICMP messages.

Examples

```
-> icmp echo reply enable
-> icmp echo enable
-> icmp echo request enable
-> icmp echo request min-pkt-gap 50
```

Release History

Release 7.1.1; command introduced

Related Commands

show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp timestamp

Enables or disables ICMP timestamp messages, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp timestamp [request | reply] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

request	Specifies timestamp request messages.
reply	Specifies timestamp reply messages.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**enable**
gap	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The data received (a timestamp) in the message is returned in the reply together with an additional timestamp. The timestamp is 32 bits of milliseconds since midnight UT. The Originate timestamp is the time the sender last touched the message before sending it, the Receive timestamp is the time the echoer first touched it on receipt, and the Transmit timestamp is the time the echoer last touched the message on sending it.
- Using this command without specifying a request or reply enables, disables, or sets the minimum packet gap for both types.
- The timestamp ICMP messages can also be enabled, disabled, and modified using the **icmp type** command. See the **icmp type** command information on the type and code for the timestamp ICMP messages.

Examples

```
-> icmp timestamp reply enable
-> icmp timestamp enable
-> icmp timestamp request enable
-> icmp timestamp request min-pkt-gap 50
```

Release History

Release 7.1.1; command introduced

Related Commands

show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp addr-mask

Enables or disables ICMP address mask messages, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp add-mask [request | reply] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

request	Specifies request address mask messages.
reply	Specifies reply address mask messages.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**enable**
gap	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- A gateway receiving an address mask request must return it with the address mask field set to the 32-bit mask of the bits identifying the subnet and network, for the subnet on which the request was received.
- Using this command without specifying a request or reply enables, disable, or set the minimum packet gap for both types.
- The address mask ICMP messages can also be enabled, disabled, and modified using the **icmp type** command. See the **icmp type** command information on the type and code for the address mask ICMP messages.

Examples

```
-> icmp addr-mask reply enable
-> icmp addr-mask enable
-> icmp addr-mask request enable
-> icmp addr-mask request min-pkt-gap 50
```

Release History

Release 7.1.1; command introduced

Related Commands

show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
```

icmp messages

Enables or disables all Internet Control Message Protocol (ICMP) messages.

icmp messages {enable | disable}

Syntax Definitions

enable	Enables ICMP messages.
disable	Disables ICMP messages.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> icmp messages enable
-> icmp messages disable
```

Release History

Release 7.1.1; command introduced

Related Commands

icmp type	Enables or disables a specific type of ICMP message, and sets the minimum packet gap.
show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrl
   alaIcmpAllMsgStatus
```

ip dos scan close-port-penalty

Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP or UDP packet is received on a closed port.

ip dos scan close-port-penalty *penalty_value*

Syntax Definitions

penalty_value	A penalty value added to the penalty scan value. This value can be any non-negative integer.

Defaults

parameter	default
penalty_value	10

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command creates a point value that is added to the total port scan penalty value when a TCP or UDP packet is received that is destined for a closed port.

Examples

```
-> ip dos scan close-port-penalty 25
```

Release History

Release 7.1.1; command introduced

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value, at which a DoS attack is recorded.
ip dos trap	Sets whether the switch generates SNMP DoS traps when an attack is detected.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanClosePortPenalty
```

ip dos scan tcp open-port-penalty

Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP packet is received on an open port.

ip dos scan tcp open-port-penalty *penalty_value*

Syntax Definitions

penalty_value	A penalty value added to the penalty scan value. This value can be any non-negative integer.

Defaults

parameter	default
penalty_value	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command creates a point value that is added to the total port scan penalty value when a TCP packet is received that is destined for an open port.
- The switch does not distinguish between a legal TCP packet and a port scan packet.

Examples

```
-> ip dos scan tcp open-port-penalty 10
```

Release History

Release 7.1.1; command introduced

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value, at which a DoS attack is recorded.
ip dos trap	Sets whether the switch generates SNMP DoS traps when an attack is detected.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanTcpOpenPortPenalty
```

ip dos scan udp open-port-penalty

Assigns a penalty value to be added to the Denial of Service penalty scan value when a UDP packet is received on an open port.

ip dos scan udp open-port-penalty *penalty_value*

Syntax Definitions

penalty_value	A penalty value added to the penalty scan value. This value can be any non-negative integer.

Defaults

parameter	default
penalty_value	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command creates a point value that is added to the total port scan penalty value when a UDP packet is received that is destined for an open port.
- The switch does not distinguish between a legal UDP packet and a port scan packet.

Examples

```
-> ip dos scan udp open-port-penalty 15
```

Release History

Release 7.1.1; command introduced

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value, at which a DoS attack is recorded.
ip dos trap	Sets whether the switch generates SNMP DoS traps when an attack is detected.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanUdpOpenPortPenalty
```

ip dos scan threshold

Sets the threshold for the port scan value, at which a DoS attack is recorded.

ip dos scan threshold *threshold_value*

Syntax Definitions

threshold_value	A numerical value representing the total acceptable penalty before a DoS attack is noted. This value can be any non-negative integer.

Defaults

parameter	default
threshold_value	1000

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the total port scan penalty value exceeds this value, a port scan attack is recorded.
- The penalty value is incremented by recording TCP or UDP packets that are bound for open or closed ports. Such packets are given a penalty value, which are added. The commands for setting the packet penalty value are the **ip dos scan close-port-penalty**, **ip dos scan tcp open-port-penalty**, and **ip dos scan udp open-port-penalty** commands.

Examples

```
-> ip dos scan threshold 1200
```

Release History

Release 7.1.1; command introduced

Related Commands

ip dos scan close-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP or UDP packet is received on a closed port.
ip dos scan tcp open-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP packet is received on an open port.
ip dos scan udp open-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a UDP packet is received on an open port.
show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanThreshold
```

ip dos trap

Sets whether or not the switch generates SNMP DoS traps when an attack is detected.

ip dos trap {enable | disable}

Syntax Definitions

enable	Enables the generation of DoS traps.
disable	Disables the generation of DoS traps.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command controls whether the switch generates an SNMP trap when a DoS attack is detected. It is assumed a DoS attack has occurred when the port scan penalty threshold is exceeded. This value is set using the **ip dos scan threshold** command.

Examples

```
-> ip dos trap enable
-> ip dos trap disable
```

Release History

Release 7.1.1; command introduced

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value, at which a DoS attack is recorded.
show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

```
alaDoSConfig
   alaDoSTrapCnt1
```

ip dos scan decay

Sets the decay speed of the port scan penalty value for the switch when calculating DoS attacks.

ip dos scan decay *decay_value*

Syntax Definitions

decay_value	The decay value amount for reducing the port scan penalty. This value can be any non-negative integer.

Defaults

parameter	default
decay_value	2

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The port scan penalty value is reduced every minute by dividing by the amount set in using this command. For example, if the decay value is set to 10, every minute the total port scan penalty value is divided by 10.

Examples

```
-> ip dos scan decay 10
```

Release History

Release 7.1.1; command introduced

Related Commands

ip dos scan threshold	Sets the threshold for the port scan value, at which a DoS attack is recorded.
show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

```
alaDoSConfig
   alaDoSPortScanDecay
```

ip dos type

Enables or disables detection for the specified type of DoS attack.

ip dos type {port-scan | ping-of-death | land | loopback-src | invalid-ip | invalid-multicast | unicast-ip-mcast-mac | ping-overload | arp-flood | arp-poison} admin-state {enable | disable}

Syntax Definitions

port-scan	Detects port scans by monitoring TCP or UDP packets sent to open or closed ports.
ping-of-death	Detects the number of ICMP Ping-of-Death attacks (the switch receives ping packets that exceed the largest IP datagram size of 65535 bytes).
land	Detects the number of Land attacks (the switch receives spoofed packets with the SYN flag set on any open port that is listening).
loopback-src	Detects the number of loopback source attacks (the switch receives packets with 127.0.0.0/8 as the IP source address).
invalid-ip	Detects invalid IP packets (the switch receives packets with an invalid source or destination IP address).
invalid-multicast	Detects invalid Multicast packets (the switch receives packets with an invalid multicast address).
unicast-ip-mcast-mac	Detects a unicast IP and multicast MAC mismatch (the switch receives IP packets with multicast/broadcast source mac-address, non-matching destination IP and mac-address).
ping-overload	Detects a ping overload attack (the switch is flooded with a large number of ICMP packets).
arp-flood	Detects ARP flooding (the switch is flooded with a large number of ARP requests).
arp-poison	Detects ARP poisoning (the switch receives replies to an ARP request generated by the switch for a user-specified restricted address).
enable	Enables DoS attack detection.
disable	Disables DoS attack detection.

Defaults

By default, detection is enabled for all the specified IP DoS attack types, except for ping overload.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When detection is enabled for ping overload, the attack is not detected until the number of ICMP packets received exceeds 100 packets-per-second.
- ARP flooding is rate limited to 500 packets-per-second on the switch. As a result, ARP flooding is not detected until the number of ARP requests exceeds 500 packets-per-second.

- When detection is enabled for unicast IP/multicast MAC mismatches (**unicast-ip-mcast-mac**), ping overload attacks (**ping-overload**), or ARP flooding attacks (**arp-flood**), packets are not dropped when the attack is detected.

Examples

```
-> ip dos type ping-overload admin-state enable
-> ip dos type land admin-state disable
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip dos config	Displays the DoS scan configuration for the switch.
show ip dos statistics	Displays statistics for the detected DoS attacks.

MIB Objects

```
alaDoSTable
   alaDoSType
   alaDoSStatus
```

ip tcp half-open-timeout

Configures the timeout periods for dropping half-open TCP connections.

ip tcp half-open-timeout *timeout_value*

Syntax Definitions

timeout_value	The timeout value in seconds. Current supported values are 3, 7, 15, 31 and 63.

Defaults

parameter	default
timeout_value	63 seconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ip tcp half-open-timeout 7
```

Release History

Release 8.4.1; command introduced

Related Commands

show ip tcp half-open-timeout	Displays the timeout value configured for half-open TCP sessions.

MIB Objects

```
systemServices
   systemServicesTcpHalfOpenTimeout
```

show ip traffic

Displays IP datagram traffic and errors.

show ip traffic

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The statistics show the cumulative totals since the last time the switch was powered on or since the last reset of the switch was executed.
- Packets received on a port that is a member of the UserPorts group are dropped if they contain a source IP network address that does not match the IP subnet for the port. This is done to block spoofed IP traffic. If the UserPorts group function is active and spoofed traffic was detected and blocked, the output display of this command includes statistics regarding the spoofed traffic.
- The presence of spoofing event statistics in the output display of this command indicates that an attack was prevented, not that the switch is currently under attack.
- If statistics for spoofed traffic are not displayed, then a spoofing attempt has not occurred since the last time this command was issued.

Examples

```
-> show ip traffic

IP statistics
  Datagrams received
    Total                   =   621883,
    IP header error         =        0,
    Destination IP error    =    51752,
    Unknown protocol        =        0,
    Local discards          =        0,
    Delivered to users      =   567330,
    Reassemble needed       =        0,
    Reassembled             =        0,
    Reassemble failed       =        0

  Datagrams sent
    Fowarded                =     2801,
    Generated               =   578108,
    Local discards          =        0,
    No route discards       =        9,
```

```
Fragmented              =     2801,
Fragment failed         =        0,
Fragments generated     =        0
```

output definitions

Total	Total number of input datagrams received including the datagrams received in the error.
IP header error	Number of IP datagrams discarded due to errors in the IP header (for example, bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discarded in processing IP options).
Destination IP error	Number of IP datagrams discarded because the IP header destination field contained an invalid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E).
Unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Local discards	Number of IP datagrams received that were discarded, even though they had no errors to prevent transmission (for example, lack of buffer space). This does not include any datagrams discarded while awaiting reassembly. This value must be zero.
Delivered to users	Total number of datagrams received that were successfully delivered to IP user protocols (including ICMP).
Reassemble needed	Number of IP fragments received that needed to be reassembled.
Reassembled	Number of IP datagrams received that were successfully reassembled.
Reassemble failed	Number of IP failures detected by the IP reassembly algorithm for all reasons (for example, timed out, error). This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragmented	Number of successfully fragmented IP datagrams.
Fragment failed	Number of packets received and discarded by IP that were not fragmented. This situation can happen if a large packet has the “Don’t Fragment” flag set.
Forwarded	Number of IP datagrams forwarded by the switch.
Generated	Total number of IP datagrams that local IP user protocols (including ICMP) generated in response to requests for transmission. This does not include any datagrams counted as “Forwarded.”
Local discards	Number of output IP datagrams that were discarded, even though they had no errors to prevent transmission (for example, lack of buffer space). This number includes datagrams counted as “Forwarded” if the packets are discarded for these reasons.
No route discards	Number of IP datagrams received and discarded by IP because no route could be found to transmit them to their destination. This includes any packets counted as “Forwarded” if the packets are discarded for these reasons. It also includes any datagrams that a host cannot route because all of its default routers are down.

output definitions (continued)

Fragments generated	The of IP datagram fragments generated as a result of fragmentation.
Routing entry discards	Number of packets received and discarded by IP even though no problems were encountered to prevent their transmission to their destination (for example, discarded because of lack of buffer space).

Release History

Release 7.1.1; command introduced

Related Commands

show icmp statistics	Displays ICMP statistics and errors.

MIB Objects

N/A

show ip interface

Displays the configuration and status of IP interfaces.

show ip interface [*if_name* **| vlan** *vlan_id* | **dhcp-client]**

Syntax Definitions

if_name	The name associated with the IP interface.
vlan_id	VLAN ID (displays a list of IP interfaces associated with a VLAN).
dhcp-client	Displays the configuration and status of a DHCP Client interface.

Defaults

By default, all IP interfaces are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the optional **vlan** parameter to display a list of interfaces configured for the specified VLAN.
- Use the optional *if_name* parameter to display detailed information about an individual interface.
- Use the optional **dhcp-client** parameter to display detailed information about an interface that has been configured to obtain an IP address from a DHCP server.
- In a virtual chassis environment this command does not accurately reflect the status of the EMP IP interface on other chassis when entered on a Slave chassis.

Examples

```
-> show ip interface
Total 13 interfaces
 Flags (D=Directly-bound)

          Name         IP Address    Subnet Mask   Status Forward Device      Flags
----------------------+-------------+-------------+------+-------+-----------+-----
EMP                   172.22.16.115 255.255.255.0     UP      NO EMP
UNP-RULE              40.1.1.1      255.255.255.0   DOWN      NO vlan 40
Loopback              127.0.0.1     255.0.0.0         UP      NO Loopback
L3VPN-2000            11.1.1.1      255.255.255.0     UP     YES service 1
L3VPN-1000            47.1.1.1      255.255.255.0     UP     YES service 2
if222                 30.1.5.1      255.0.0.0         UP     YES vlan 222
ldap_client1          173.22.16.115 255.255.255.0     UP     YES vlan 173
ldap_server1          174.22.16.115 255.255.255.0     UP     YES vlan 174
radius_client3        110.1.1.101   255.255.255.0     UP     YES vlan 30
vlan-2                0.0.0.0       0.0.0.0         DOWN      NO unbound
gre-1                 24.24.24.1    255.255.255.0     UP     YES GRE tunnel
ipip-1                25.25.25.1    255.255.255.0     UP     YES IPIP tunnel
rp-vlan850            37.2.2.1      255.0.0.0       DOWN      NO vlan 850     D
vlan-23               23.23.23.1    255.255.255.0     UP     YES vlan 23
```

output definitions

Name	Interface name. This is the name configured for the interface (for example, Accounting). **EMP-CMMA-CHAS1** refers to the Ethernet Management Port. **Loopback** refers to a built-in loopback interface that provides a local host address for the switch.
IP Address	IP address of the interface. Configured through the **ip interface** command.
Subnet Mask	IP subnet mask for the interface IP address. Configured through the **ip interface** command.
Status	Interface status: • **UP**—Interface is ready to pass packets. • **DOWN**—Interface is down.
Forward	Indicates whether the interface is actively forwarding packets (**YES** or **NO**).
Device	The type of device bound to the interface: • **unbound**—No device is bound to the interface. • **vlan**—The VLAN ID that is bound to the interface. • **EMP**—The Ethernet Management Port is bound to the interface. • **Loopback**—A loopback interface is configured for testing. • **GRE tunnel**—GRE tunnel is configured for the interface. • **IPIP tunnel**—IPIP tunnel is configured for the interface. • **service**—The service ID that is bound to this interface. Configured through the **ip interface** command.
Flags	Indicates if a switch port or link aggregate is directly bound to the interface (**D**=Directly-bound). This flag displays for IP routed-port interfaces.

```
-> show ip interface vlan-23
Interface Name = vlan-23
  SNMP Interface Index          =   13600007,
  IP Address                    =   23.23.23.1,
  Subnet Mask                   =   255.0.0.0,
  Broadcast Address             =   23.255.255.255,
  Device                        =   vlan 23,
  Encapsulation                 =   eth2,
  Forwarding                    =   enabled,
  Administrative State          =   enabled,
  Operational State             =   up,
  Maximum Transfer Unit         =   1500,
  ARP Count                     =   1,
  Router MAC                    =   2c:fa:a2:13:e4:02,
  Local Proxy ARP               =   disabled,
  Primary (config/actual)       =   no/yes

-> show ip interface L3VPN
Interface Name = L3VPN
  SNMP Interface Index          =   13600003,
  IP Address                    =   47.1.1.1,
  Subnet Mask                   =   255.255.255.0,
  Broadcast Address             =   47.1.1.255,
  Device                        =   Service 1,
  Forwarding                    =   enabled,
  Administrative State          =   enabled,
  Operational State             =   up,
  Maximum Transfer Unit         =   1500,
```

```
  Router MAC                      =   e8:e7:32:1d:4c:88

-> show ip interface rp-vlan850
Interface Name = rp-vlan850
  SNMP Interface Index            =   13600004,
  IP Address                      =   37.2.2.1,
  Subnet Mask                     =   255.0.0.0,
  Broadcast Address               =   37.255.255.255,
  Device                          =   vlan 850,
  Encapsulation                   =   eth2,
  Forwarding                      =   disabled,
  Administrative State            =   enabled,
  Operational State               =   down,
  Operational State Reason        =   device-down,
  Maximum Transfer Unit           =   1500,
  ARP Count                       =   0,
  Router MAC                      =   00:e0:b1:e7:09:a3,
  Local Proxy ARP                 =   disabled,
  Primary (config/actual)         =   no/no
  Directly bound port             =   1/1/2, tagged

-> show ip interface dhcp-client
Interface Name = dhcp-client
  SNMP Interface Index            =   13600010,
  IP Address                      =   0.0.0.0,
  Subnet Mask                     =   0.0.0.0,
  Broadcast Address               =   0.0.0.0,
  Device                          =   vlan 1,
  Encapsulation                   =   eth2,
  Forwarding                      =   disabled,
  Administrative State            =   enabled,
  Operational State               =   down,
  Operational State Reason        =   unbound,
  Maximum Transfer Unit           =   1500,
  ARP Count                       =   0,
  Router MAC                      =   2c:fa:a2:7a:a7:db,
  Local Proxy ARP                 =   disabled,
  Primary (config/actual)         =   yes/yes
  Vsi Accept Filter               =   ,

DHCP-CLIENT Parameter Details
  Dhcp Prefer Server              =   FALSE,
  Client Status                   =   Discovery,
  Server IP                       =   N.A.,
  Router Address                  =   N.A.,
  Lease Time Remaining            =   N.A.,
  Option-60                       =   OmniSwitch-OS6560-P48Z16,
  HostName                        =   OS6560,
```

output definitions

SNMP Interface Index	Interface index.
IP Address	IP address associated with the interface. Configured through the **ip interface** command.
Subnet Mask	IP subnet mask for the interface. Configured through the **ip interface** command.
Broadcast Address	Broadcast address for the interface.

output definitions (continued)

Device	The type of device bound to the interface: • **unbound**—No device is bound to the interface. • **vlan**—The VLAN ID that is bound to the interface. • **EMP**—The Ethernet Management Port is bound to the interface. • **Loopback**—A loopback interface is configured for testing. • **GRE tunnel**—GRE tunnel is configured for the interface. • **IPIP tunnel**—IPIP tunnel is configured for the interface. • **service**—The service ID that is bound to this interface. Configured through the **ip interface** command.
Encapsulation	Displays the IP router encapsulation (**eth2** or **snap**) that the interface uses when routing packets. Configured through the **ip interface** command.
Forwarding	Indicates whether IP forwarding is active for the interface (**enabled** or **disabled**). Configured through the **ip interface** command.
Administrative State	Administrative state of the IP interface (**enabled** or **disabled**), which is independent of the state of the underlying device. Configured through the **ip interface** command.
Operational State	Indicates whether the interface is active (**up** or **down**).
Operation State Reason	Indicates why the operational state of the interface is down: • **unbound**—No device is bound to the interface. • **device-down—**Device bound to the interface is down. • **admin-down—**The admin state of the interface is down. • **no-such-device—**Device does not exist. • **no-router-mac—**No MAC address available for the interface. • **tunnel-src-invalid—**The source IP address of the tunnel is invalid. • **tunnel-dst-unreachable—**The destination IP address of the tunnel is not reachable. The **tunnel-src-invalid** and **tunnel-dst-unreachable** Operational State reasons apply only when the type of device bound to the interface is a **GRE tunnel** or **IPIP tunnel**. **Operational State Reason** field is only included in the display output when the operational state of the interface is **down**.
Maximum Transfer Unit	The Maximum Transmission Unit size set for the interface. Configured through the **vlan mtu-ip** command.
Router MAC	Switch MAC address assigned to the interface. Each interface assigned to the same VLAN shares the same switch MAC address.
Local Proxy ARP	Indicates whether Local Proxy ARP is active for the interface (**enabled** or **disabled**). Configured through the **ip interface** command.
Primary (config/actual)	Indicates if the interface is the configured and/or actual primary interface for the device (VLAN, EMP, Loopback). If the actual status is set to **yes** and the config status is set to **no**, the interface is the default interface for the VLAN. Configured through the **ip interface** command.
Directly bound port	Displays the physical port or link aggregate that is directly bound to the interface. Configured through the **ip interface rtr-port** command. This field displays only when the interface is configured as an IP routed port interface.
ARP Count	Displays the number of ARP entries in the NI.
DHCP-Client Parameter Details	(The following parameters are only applicable to the 'dhcp-client' interface. Configured through the **ip interface dhcp-client** command.)

output definitions (continued)

Dhcp Prefer Server	Indicates if the DHCP server preference option is enabled or disabled.
Client Status	DHCP Client Status (**In-active**, **Active**)
Server IP	The IP address of the DHCP server.
Router Address	The IP address of the DHCP router.
Lease Time Remaining	The lease time remaining for the DHCP client IP address.
Option-60	The option-60 string that will be included in DHCP discover or request packets.
HostName	The system name of the OmniSwitch.

```
-> show ip interface ipip-1
Interface Name = ipip-1
  SNMP Interface Index           =   13600001,
  IP Address                     =   25.25.25.1,
  Subnet Mask                    =   255.255.255.0,
  Device                         =   IPIP Tunnel,
  Tunnel Source Address          =   23.23.23.1
  Tunnel Destination Address     =   23.23.23.2,
  Forwarding                     =   enabled,
  Administrative State           =   enabled,
  Operational State              =   up,
  Maximum Transfer Unit          =   1480,

-> show ip interface gre-1
Interface Name = gre-1
  SNMP Interface Index           =   13600002,
  IP Address                     =   24.24.24.1,
  Subnet Mask                    =   255.255.255.0,
  Device                         =   GRE Tunnel,
  Tunnel Source Address          =   23.23.23.1
  Tunnel Destination Address     =   23.23.23.2,
  Forwarding                     =   enabled,
  Administrative State           =   enabled,
  Operational State              =   down,
  Operational State Reason       =   unbound,
  Maximum Transfer Unit          =   1476,
```

output definitions

SNMP Interface Index	Interface index.
IP Address	IP address associated with the interface. Configured through the **ip interface** command.
Subnet Mask	IP subnet mask for the interface. Configured through the **ip interface** command.
Device	The type of device bound to the interface: • **unbound**—No device is bound to the interface. • **vlan**—The VLAN ID that is bound to the interface. • **EMP**—The Ethernet Management Port is bound to the interface. • **Loopback**—A loopback interface is configured for testing. • **GRE tunnel**—GRE tunnel is configured for the interface. • **IPIP tunnel**—IPIP tunnel is configured for the interface. • **service**—The service ID that is bound to this interface. Configured through the **ip interface** command.

output definitions (continued)

Tunnel Source Address	The source IP address for the tunnel.
Tunnel Destination Address	The destination IP address for the tunnel.
Forwarding	Indicates whether IP forwarding is active for the interface (**enabled** or **disabled**). Configured through the **ip interface** command.
Administrative State	Administrative state of the IP interface (**enabled** or **disabled**), which is independent of the state of the underlying device. Configured through the **ip interface** command.
Operational State	Indicates whether the interface is active (**up** or **down**).
Operational State Reason	Indicates why the operational state of the interface is down: • **interface-up—**The admin state of the interface is up. • **unbound**—No device is bound to the interface. • **device-down—**Device bound to the interface is down. • **admin-down—**The administrative state of the interface is down. • **no-such-device—**Device does not exist. • **no-router-mac—**No MAC address available for the interface. • **tunnel-src-invalid—**The source IP address of the tunnel is invalid. • **tunnel-dst-unreachable—**The destination IP address of the tunnel is not reachable. **Operational State Reason** field is only included in the display output when the operational state of the interface is **down**.
Maximum Transfer Unit	The Maximum Transmission Unit size set for the interface. Configured through the **vlan mtu-ip** command.

Release History

Release 7.1.1; command introduced
Release 7.3.4; output modified to display **Designated NI** and **ARP Count**.
Release 8.5R1; **Dhcp prefer server** field added in output.

Related Commands

ip interface	Configures an IP interface to enable IP routing on a VLAN. Without an IP interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.
ip interface tunnel	Configures the end points for the GRE and IPIP tunnels.
show ip emp-interfaces	Displays the configuration and status of the Ethernet Management Port (EMP) interface.
show icmp statistics	Displays ICMP statistics and errors.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   alaIpInterfaceIpForward
   alaIpInterfaceEncap
   alaIpInterfaceLocalProxyArp
   alaIpInterfacePrimCfg
   alaIpInterfaceOperState
   alaIpInterfaceOperReason
   alaIpInterfaceRouterMac
   alaIpInterfaceBcastAddr
   alaIpInterfacePrimAct
   alaIpInterfaceMtu
   alaIpInterfaceTunnelSrc
   alaIpInterfaceTunnelDst
   alaIpInterfaceArpCount
   alaIpInterfacePortIfindex
   alaIpInterfaceTag
```

show ip emp-interfaces

Displays the configuration and status of the Ethernet Management Port (EMP) interface.

show ip emp-interfaces

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **show ip emp-routes** to display IP routes associated with the EMP interface.

Examples

```
-> show ip emp-interfaces
Total 1 interfaces
 Flags (D=Directly-bound)

          Name         IP Address    Subnet Mask   Status Forward Device      Flags
----------------------+-------------+-------------+------+-------+-----------+-----
EMP-CMMA-CHAS1         3.3.3.25      255.0.0.0       DOWN      NO EMP
```

Name	Interface name. **EMP-CMMA-CHAS1** refers to the Ethernet Management Port.
IP Address	IP address of the interface. Configured through the **ip interface** command.
Subnet Mask	IP subnet mask for the interface IP address. Configured through the **ip interface** command.
Status	Interface status: • **UP**—Interface is ready to pass packets. • **DOWN**—Interface is down.
Forward	Indicates whether the interface is actively forwarding packets (**YES** or **NO**).
Device	**EMP**—The Ethernet Management Port is bound to the interface.
Flags	N/A for EMP interfaces.

Release History

Release 7.3.3; command introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

N/A

show ip routes

Displays the IP Forwarding table.

[vrf *vrf_name***] show ip routes [summary]**

Syntax Definitions

vrf_name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
summary	Displays a summary of routing protocols that appear in the IP Forwarding table.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The IP Forwarding table includes static routes as well as all routes learned through routing protocols (for example, RIP, OSPF).
- Use the optional **summary** keyword to display a list of routing protocols and the number of routes for each protocol that appear in the IP Forwarding table.
- The imported routes are also displayed under the protocol field as IMPORT in the show output.

Examples

```
-> show ip routes

+ = Equal cost multipath routes
 Total 4 routes

  Dest Address      Gateway Addr        Age       Protocol
------------------+-----------------+---------+-----------
  0.0.0.0/0          10.255.11.254     01:50:33   STATIC
  10.255.11.0/24     10.255.11.225     01:50:33   LOCAL
  127.0.0.1/32       127.0.0.1         01:51:47   LOCAL
  212.109.138.0/24   212.109.138.138   00:33:07   LOCAL
  12.0.0.0/8         12.0.0.1          00:20:00   IMPORT
  55.0.0.0/8         0.0.0.0           00:00:17   STATIC

-> show ip route summary

  Protocol        Route Count
----------------+--------------
  Local                    3
  Static                   2
  RIP                      0
  ISIS                     0
```

```
OSPF                    0
BGP                     0
Import                  1
Other                   0

TOTAL =                 6
```

output definitions

Dest Addr	Destination IP address/mask length.
Gateway Addr	IP address of the gateway from which this address was learned. Gateway address ‘0.0.0.0’ indicates an IPv4 blackhole route.
Age	Age of the entry. If the entry is less than a day old, it is displayed in *hh/mm/ss* format. If it is more than a day old, it is displayed in *dd/hh* format (for example, a route that is 2 days and 12 hours old is displayed as 2d12h).
Protocol	Protocol by which this IP address was learned (for example, RIP). LOCAL indicates a local interface.
Route Count	The number of routes that appear in the IP Forwarding table for each protocol type listed.

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** parameter added.

Related Commands

ping	Used to test whether an IP destination can be reached from the local switch.
traceroute	Used to find the path taken by an IP packet from the local switch to a specified destination.
show ip router database	Displays a list of all routes (static and dynamic) that exist in the IP router database.

MIB Objects

```
ipCidrRouteTable
   ipCidrRouteDest
   ipCidrRouteMask
   ipCidrRouteTos
   ipCidrRouteNextHop
   ipCidrRouteIfIndex
   ipCidrRouteType
   ipCidrRouteProto
   ipCidrRouteAge
   ipCidrRouteInfo
   ipCidrRouteNextHopAS
   ipCidrRouteMetric1
   ipCidrRouteMetric2
   ipCidrRouteMetric3
   ipCidrRouteMetric4
   ipCidrRouteMetric5
   ipCidrRouteStatus
```

show ip route-pref

Displays the IPv4 routing preferences of a router.

[vrf *vrf_name***] show ip route-pref**

Syntax Definitions

vrf_name	The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

By default, ISIS Level 1 routes are preferred over ISIS Level 2 routes and EBGP routes will carry a higher precedence than IBGP routes.

Examples

```
-> show ip route-pref
  Protocol    Route Preference Value
------------+-----------------------
  Local                 1
  Static                2
  OSPF                110
  ISISL1              115
  ISISL2              118
  RIP                 120
  EBGP                190
  IBGP                200
  Import              210
```

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** parameter added.

Related Commands

ip route-pref	Configures the route preference of a router.

MIB Objects

```
alaIprmRtPrefTable
  alaIprmRtPrefEntryType
  alaIprmRtPrefEntryValue
```

show ip redist

Displays the IPv4 route map redistribution configuration.

[vrf *vrf_name***] show ipv6 redist [rip | ospf | isis | bgp]**

Syntax Definitions

vrf_name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
rip	Displays route map redistribution configurations that use RIP as the destination (into) protocol.
ospf	Displays route map redistribution configurations that specify OSPF as the destination (into) protocol.
isis	Displays route map redistribution configurations that specify ISIS as the destination (into) protocol.
bgp	Displays the route map redistribution configurations that specify BGP as the destination (into) protocol at this time.

Defaults

By default, all route map redistribution configurations are shown.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Specify a destination protocol with this command to display only those configurations that redistribute routes into the specified protocol.

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** parameter added.

Examples

```
-> show ip redist

Source       Destination
Protocol     Protocol     Status    Route Map
-------------+------------+---------+--------------------
RIP          OSPF         Enabled   ipv4rm
BGP          RIP          Enabled   ipv4rm
IMPORT       RIP          Enabled   ipv4rm
```

```
-> show ip redist rip

Source       Destination
Protocol     Protocol     Status    Route Map
-------------+------------+---------+--------------------
BGP          RIP          Enabled   ipv4rm
IMPORT       RIP          Enabled   ipv4rm
```

output definitions

Source Protocol	The protocol from which the routes are learned.
Destination Protocol	The protocol into which the source protocol routes are redistributed.
Status	The administrative status (**Enabled** or **Disabled**) of the route map redistribution configuration.
Route Map	The name of the route map that is applied with this redistribution configuration.

Related Commands

ip redist	Controls the conditions for redistributing different IPv6 routes between protocols.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistSrcProtoId
   alaRouteMapRedistDestProtoId
   alaRouteMapRedistRouteMapIndex
   alaRouteMapRedistStatus
   alaRouteMapRedistAddressType
   alaRouteMapRedistRowStatus
```

show ip access-list

Displays the details of the access list.

show ip access-list [*access_list_name***]**

Syntax Definitions

access_list_name	Name of the access list.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the *access_list_name* is not specified in this command, all the access lists are displayed.

Examples

```
-> show ip access-list
                     Address /                  Redistribution
Name                 Prefix Length      Effect  Control
--------------------+------------------+-------+-------------
al_3                 10.0.0.0/8         permit  all-subnets
al_3                 11.0.0.0/8         permit  all-subnets
al_4                 1.0.0.0/8          permit  no-subnets
al_4                 10.0.0.0/8         permit  all-subnets

-> show ip access-list al_4

                     Address /                  Redistribution
Name                 Prefix Length      Effect  Control
--------------------+------------------+-------+-------------
al_4                 1.0.0.0/8          permit  no-subnets
al_4                 10.0.0.0/8         permit  all-subnets
```

output definitions

Name	Name of the access list.
Address/Prefix Length	IP address that belongs to the access list.
Effect	Indicates whether the IP address is permitted or denied.
Redistribution Control	Indicates the conditions specified for redistributing the matched routes.

Release History

Release 7.1.1; command was introduced

Related Commands

ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
ip access-list address	Adds multiple IPv4 addresses to the access list.

MIB objects

```
alaRouteMapAccessListIndex
alaRouteMapAccessListAddressType
alaRouteMapAccessListAddress
alaRouteMapAccessListPrefixLength
alaRouteMapAccessListAction
alaRouteMapAccessListRedistControl
```

show ip route-map

Displays the IP route maps configured on the switch.

show ip route-map [*route_map_name***]**

Syntax Definitions

route_map_name	The name of the specific route map.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the *route_map_name* is not specified in this command, all the route maps are displayed.

Examples

```
-> show ip route-map
Route Maps: configured: 1 max: 200
Route Map: Route_map1 Sequence Number: 50 Action permit
  match ip address 10.0.0.0/8 redist-control all-subnets permit
  set metric 100 effect replace
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match ip address	Matches the route with the specified IPv4 address or with addresses contained in an IPv4 access list specified by the access list name.
ip route-map match ipv6 address	Matches the route with the specified IPv6 address or with addresses contained in an IPv6 access list specified by the access list name
ip route-map match ip-nexthop	Matches the routes that have a next-hop router address permitted by the specified access list.
ip route-map match ipv6-nexthop	Matches the routes that have an IPv6 next-hop router address permitted by the specified access list
ip route-map match tag	Permits or denies a route based on the specified next-hop IP address.
ip route-map match tag	Matches the tag value specified in the route map with the one that the routing protocol learned the route on.
ip route-map match metric	Matches the metric value specified in the route map with the one that the routing protocol learned the route on.
ip route-map match route-type	Matches the specified route type with the one that the routing protocol learned the route on.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistRouteMapIndex
alaRouteMapTable
   alaRouteMapIndex
   alaRouteMapSequence
   alaRouteMapType
   alaRouteMapValue
   alaRouteMapRowStatus
```

show ip router database

Displays a list of all routes (static and dynamic) that exist in the IP router database. This database serves as a central repository where routes are first processed and where duplicate routes are compared to determine the best route for the Forwarding Routing Database. If a route does not appear in the IP router database list, then the switch does not know about it. In the case of dynamically learned routes, this could indicate that the route was never received by the switch.

[vrf *vrf_name***] show ip router database [protocol** *type* | **gateway** *ip_address* | **dest {***ip_address/prefixlen* | *ip_address***}]**

Syntax Definitions

vrf_name	The alphanumeric name (1–20 characters) assigned to the VRF instance.
type	Routing protocol type (local, static, OSPF, RIP, or BGP).
ip_address	Destination IP address.
ip_address/prefixlen	The destination IP address along with the prefix length of the routes processed for redistribution.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Command options are not mutually exclusive. You can use them on the same command line to narrow and/or customize the output display of this command. For example, use the **protocol** and **dest** options to display only those routes that are of a specific protocol type and have the specified destination network.
- The IP forwarding table is derived from IP router database processing performed by the switch and contains only unique routes that the switch currently uses. Use the **show ip route** command to view the forwarding table.
- If an expected route does not appear in the IP forwarding table, use the **show ip router database** command to see if the switch knows about the route and/or if a duplicate route with a higher precedence was selected instead.
- The switch compares the protocol of duplicate routes to determine which one to use. Regardless of whether a route has a higher priority metric value, protocol determines precedence. Local routes are given the highest level of precedence followed by static, OSFP, RIP, then BGP routes. As a result, a route that is known to the switch does not appear in the IP forwarding table if a duplicate route with a higher protocol precedence exists.
- A list of inactive static routes is also included in the **show ip router database** output display. A route becomes inactive if the interface for its gateway goes down. Inactive routes are unable to get to their destination and further investigation is warranted to determine why their gateway is unavailable.

- Static routes that appear as inactive are not included in the main IP router database listing. If an inactive route becomes active, however, it is removed from the inactive list and added to the active route list.
- The imported routes are also displayed under the protocol field as IMPORT in the show output.

Examples

```
-> show ip router database
Legend: + indicates routes in-use
        b indicates BFD-enabled static route
        r indicates recursive static route, with following address in brackets
        i indicates static interface route

Destination         Gateway         Interface   Protocol  Metric   Tag   Misc-Info
------------------+--------------+-----------+--------+---------+------+---------
+  20.0.0.0/8       20.0.0.1        ip20        LOCAL       1       0
+b 22.0.0.0/8       20.0.0.22       ip20        STATIC      4       0
   22.0.0.0/8       20.0.0.9        ip20        RIP         22      0    (backup)
+r 33.0.0.0/8       20.0.0.9        ip20        STATIC      33      0   [22.0.0.33]
+i 44.0.0.0/8       20.0.0.1        ip20        STATIC      5       0
+  127.0.0.1/32     127.0.0.1       Loopback    LOCAL       1       0
+  172.28.4.0/32    172.28.4.1      EMP         LOCAL       1       0
+  55.0.0.0/8       0.0.0.0         Loopback    STATIC      1       0

Inactive Static Routes
Destination       Gateway        Metric    Tag   Misc-Info
----------------+--------------+--------+-------+-----------
1.0.0.0/8         8.4.5.3         1         0

-> show ip router database dest 10.212.62.0/24 protocol ospf
Destination       Gateway         Interface   Protocol   Metric   Tag     Misc-Info
-----------------+--------------+-----------+----------+--------+--------+---------
10.212.62.0/24     10.212.60.27     I1          OSPF      2        0
10.212.62.0/24     10.212.61.27     I2          OSPF      2        0
```

output definitions

Destination	Destination IP address. Also includes the mask prefix length notation after the address to indicate the subnet mask value. For example, **/24** indicates the destination IP address has a 24-bit mask (255.255.255.0).
Gateway	IP address of the gateway from which this route was learned. Gateway address ‘0.0.0.0’ indicates an IPv4 blackhole route.
Interface	The interface associated with the gateway.
Protocol	Protocol by which this IP address was learned: LOCAL, STATIC, OSPF, RIP, BGP).
Metric	RIP metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.
Tag	The tag associated with the route.
Misc-Info	Any additional information about the route.

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** parameter added.

Related Commands

show ip routes	Displays the IP Forwarding table.

MIB Objects

```
alaIprmRouteTable
   alaIprmRouteDest
   alaIprmRouteMask
   alaIprmRouteTos
   alaIprmRouteNextHop
   alaIprmRouteProto
   alaIprmRouteMetric
   alaIprmRoutePriority
```

show ip emp-routes

Displays the IP routes associated with the Ethernet Management Port (EMP).

show ip emp-routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command displays the routes that are connected to the Ethernet Management Port (EMP).
- The EMP cannot handle routing protocols such as RIP or OSPF.
- The default route for the switch cannot be set up on the EMP.
- There is no dedicated routing table for the EMP interface. All management interfaces use the same routing table with EMP and non-EMP routes.

Examples

```
-> show ip emp-routes
Dest Address      Subnet Mask       Gateway Addr      Age       Protocol
------------------+-----------------+-----------------+---------+-----------
  127.0.0.1         255.255.255.255   127.0.0.1           2d 4h  LOCAL
  172.17.1.10       255.255.255.255   10.255.11.225       1d 5h  LOCAL
```

output definitions

Dest Addr	Destination IP address.
Subnet Mask	Destination IP address IP subnet mask.
Gateway Addr	IP address of the gateway from which this address was learned.
Age	Age of the entry. If the entry is less than a day old, it is displayed in *hh/mm/ss* format. If it is more than a day old, it is displayed in *dd/hh* format (for example, a route that is 2 days and 12 hours old is displayed as 2d12h).
Protocol	Protocol by which this IP address was learned (for example, RIP). NETMGT indicates a static route. LOCAL indicates a local interface.

Release History

Release 7.1.1; command introduced

Related Commands

ping	Tests whether an IP destination can be reached from the local switch.
traceroute	Finds the path taken by an IP packet from the local switch to a specified destination.

MIB Objects

N/A

show ip config

Displays IP configuration parameters.

show ip config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip config
IP directed-broadcast   =   OFF,
IP default TTL          =   64
```

output definitions

IP directed-broadcast	Indicates whether the IP directed-broadcast feature is on or off.
IP default TTL	IP default TTL interval.

Release History

Release 7.1.1; command introduced

Related Commands

ip directed-broadcast	Enables or disables IP directed broadcasts routed through the switch.
ip default-ttl	Sets TTL value for IP packets.

MIB Objects

N/A

show ip protocols

Displays switch routing protocol information and status.

show ip protocols

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip protocols
IP Protocols
RIP status                              = Not Loaded,
OSPF status                             = Loaded,
ISIS status                             = Not Loaded,
BGP status                              = Loaded,
PIM status                              = Loaded,
DVMRP status                            = Not Loaded,
RIPng status                            = Not Loaded,
OSPF3 status                            = Loaded,
```

output definitions

RIP status	Whether RIP is loaded or not.
OSPF status	Whether OSPF is loaded or not.
BGP status	Whether BGP is loaded or not.
DVMRP status	Whether DVMRP is loaded or not.
PIMSM status	Whether PIMSM is loaded or not.
RIPng status	Whether RIP is loaded or not.
OSPF3 status	Whether OSPFv3 is loaded or not.

Release History

Release 7.1.1; command introduced

Related Commands

ip interface dhcp-client	Configures the router primary IP address.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
alaIpRouteSumTable
   alaIpRouteProtocol
```

show ip router-id

Displays the primary IP address and router ID of the switch, if configured.

show ip router-id

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip router-id
Router ID    = 1.1.1.1,
Primary addr = 31.0.0.1
```

output definitions

Router ID	The set routing ID. The router ID is how the router is identified in IP.
Primary addr	The primary interface address the route uses.

Release History

Release 7.1.1; command introduced

Related Commands

ip interface dhcp-client	Configures the router primary IP address.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
alaIpRouteSumTable
   alaIpRouteProtocol
```

show ip service

Displays the status of TCP/UDP service ports.

show ip service

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The display output from this command also includes the service port number.

Examples

```
-> show ip service
Name                     Port    Status
---------------------+-------+---------
ftp                        21   enabled
ssh                        22   disabled
telnet                     23   disabled
udp-relay                  67   disabled
http                       80   disabled
network-time              123   disabled
snmp                      161   disabled
avlan-telnet              259   disabled
avlan-http                260   disabled
avlan-secure-http         261   disabled
secure_http               443   enabled
proprietary              1024   disabled
proprietary              1025   disabled
```

output definitions

Name	Name of the TCP/UDP service.
Port	The TCP/UDP well-known port number associated with the service.
Status	The status of the well-known service port: **enabled** (port is closed) or **disabled** (port is open).

Release History

Release 7.1.1; command introduced

Related Commands

ip service	Enables (opens) or disables (closes) well-known TCP/UDP service ports.

MIB Objects

```
alaIpServiceTable
   alaIpServiceType
   alaIpServicePort
   alaIpServiceStatus
alaIpPortServiceTable
   alaIpPortServicePort
   alaIpPortServiceStatus
```

show ip service source-ip

Displays the source IP interfaces configured for the applications.

[vrf *vrf_name***] show ip service source-ip**

Syntax Definitions

vrf_name	Name of the VRF.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip service source-ip
Legend: "-"denotes no explicit configuration.

Application         Interface-name
------------------+----------------------
dns                   -
ftp                  ipVlan100
ldap                 Loopback0
ntp                  Loopback0
radius               Loopback0
sflow                  -
snmp                 Loopback0
ssh                  ipVlan100
swlog                  -
tacacs                 -
telnet                 -
tftp                 ipVlan100
```

output definitions

Application	Name of the TCP/UDP service.
Interface-name	The source IP configured for the application.

Release History

Release 7.3.4; command introduced

Related Commands

ip service source-ip	Configures a user-defined source IP address as the outgoing IP interface for the IP service.

MIB Objects

```
alaIpServiceSourceIPTable
   alaIPServiceSourceIpAppIndex
   alaIPServiceSourceIpNane
   alaIpServiceSourceIpRowStatus
```

show ip dos arp-poison

Displays the number of attacks detected for configured ARP poison restricted-addresses.

show ip dos arp-poison

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip dos arp-poison
 IP Address                          Attacks
-------------------------------------+------------
192.168.1.1                             0
192.168.1.2                             0
192.168.1.3                             0
```

output definitions

IP Address	The configured ARP Poison restricted-addresses.
Attacks detected	The number of ARP Poison attacks detected for each address.

Release History

Release 7.1.1; command introduced

Related Commands

ip dos arp-poison restricted-address	Adds or deletes an ARP Poison restricted address.

MIB Objects

```
alaDoSArpPoisonTable
   alaDoSArpPoisonIpAddr
   alaDoSArpPoisonDetected
```

show arp

Displays the ARP table. The ARP table contains a listing of IP addresses and their corresponding translations to physical MAC addresses.

show arp [*ip_address* **|** *mac_address***]**

Syntax Definitions

ip_address	IP address of the entry you want to view.
mac_address	MAC address of the entry you want to view.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the basic command (**show arp**) to view all of the entries in the table. Enter a specific IP address or MAC address to view a specific entry.

Examples

```
-> show arp
Total 8 arp entries
 Flags (P=Proxy, A=Authentication, V=VRRP, R=Remote, B=BFD, H=HAVLAN, I=Interface)

 IP Addr           Hardware Addr       Type       Flags   Port     Interface
-----------------+-------------------+----------+-------+-------------+----------
 10.255.11.59      00:50:04:b2:c9:ee   DYNAMIC                   3/20  vlan 1
 10.255.11.48      00:50:04:b2:ca:11   DYNAMIC                   3/20  vlan 1
 10.255.11.201     00:10:83:03:e7:e4   DYNAMIC                   3/20  vlan 1
 10.255.11.14      00:10:5a:04:19:a7   DYNAMIC                   3/20  vlan 1
 10.255.11.64      00:b0:d0:62:fa:f1   DYNAMIC                   3/20  vlan 1
 10.255.11.25      00:b0:d0:42:80:24   DYNAMIC                   3/20  vlan 1
 10.255.11.26      00:b0:d0:42:82:59   DYNAMIC                   3/20  vlan 1
 20.0.0.22         e4:c2:33:00:21:12   STATIC      I             1/20  ip20
 10.255.11.254     00:20:da:db:00:47   DYNAMIC                   3/20  vlan 1
 11.1.1.2          e2:e7:32:1e:4b:f8   DYNAMIC             sap:2/1:200  L3VPN-2000
 11.1.1.3          e2:e7:32:1e:3b:f1   DYNAMIC           sdp:32768:200  L3VPN-2000
```

output definitions

IP Address	Device IP address.
Hardware Addr	MAC address of the device that corresponds to the IP address.
Type	Indicates whether the ARP cache entries are dynamic or static.

output definitions (continued)

Flags	Indicates the type of entry: • P = Proxy • A = Authentication (AVLAN) • V = VRRP • R = Remote • B = BFD • H = HAVLAN • I = Interface
Port	The port on the switch attached to the device identified by the IP address.
Interface	The interface to which the entry belongs (for example, VLAN, EMP).

Release History

Release 7.1.1; command introduced

Related Commands

ip service	Adds a permanent entry to the ARP table.
ip distributed-arp admin-state	Deletes all dynamic entries from the ARP table.

MIB Objects

```
ipNetToMediaTable
   ipNetToMediaIfIndex
   ipNetToMediaNetAddress
   ipNetToMediaPhyAddress
   ipNetToMediaType
ipNetToMediaAugTable
   ipNetToMediaSlot
   ipNetToMediaPort
alaIpNetToMediaTable
   alaIpNetToMediaPhyAddress
   alaIpNetToMediaProxy
   alaIpNetToMediaVRRP
   alaIpNetToMediaAuth
```

show ip arp utilization

Displays the designated NIs for the interfaces and the NI utilization.

show ip arp utilization [slot *chassis*/*slot* | **interfaces]**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number of the interface. The output is displayed specific to the slot.
interfaces	Displays the ARP utilization of the designated-NI on all the configured interfaces.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

Use the basic command (**show ip arp utilization**) to view all of the entries in the table. Enter a specific chassis and slot number to view a specific entry.

Examples

```
-> show ip arp utilization
Distributed ARPs:  Enabled
                   ARP     HW
  NI     Max     Count   Usage    %
------+--------+-------+-------+-------
1/1      16384       8      11    0%
2/1      16384      12      15    0%

-> show ip arp utilization interfaces
Distributed ARPs:  Enabled
                   ARP     HW
  NI     Max     Count   ARPS     %      VRF       Interface
------+--------+-------+-------+-------+------+-----------------
1/1      16384       1       0    0%      0    15
1/1      16384       5       4    0%      0    16
1/1      16384       5       0    0%      0    17
1/1      16384       5       4    0%      0    18
1/1      16384       5       0    0%      0    19
1/1      16384       5       0    0%      0    20
2/1      16384       1       0    0%      0    15
2/1      16384       5       0    0%      0    16
2/1      16384       5       4    0%      0    17
2/1      16384       5       0    0%      0    18
2/1      16384       5       4    0%      0    19
2/1      16384       5       4    0%      0    20
```

```
-> show ip arp utilization slot 2/1
Distributed ARPs:  Enabled
                  ARP     HW
  NI      Max     Count   ARPS     %      VRF       Interface
------+--------+-------+-------+------+------+-----------------
2/1      16384       1       0    0%      0    15
2/1      16384       5       0    0%      0    16
2/1      16384       5       4    0%      0    17
2/1      16384       5       0    0%      0    18
2/1      16384       5       4    0%      0    19
2/1      16384       5       4    0%      0    20
```

output definitions

NI	The chassis and slot number of the designated-NI.
Max	The maximum number of ARP entries supported on the NI.
ARP count	ARP count in the NI for the NI or interface.
HW Usage	The amount of table space used up in the ASIC.
HW ARPS	The number of ARPs in the ASIC.
%	The percentage of ARP utilization on that designated-NI.
VRF	The name of the VRF associated to the interface.
Interface	The interface to which the entry belongs.

Release History

Release 7.3.4; command introduced

Related Commands

ip distributed-arp admin-state Enables or disables the distributed ARP feature.

MIB Objects

```
alaDistArpNiTable
   alaDistArpItfTable
```

show arp filter

Displays a list of ARP filters configured for the switch.

show arp filter [*ip_address***]**

Syntax Definitions

ip_address	IP address of the filter entry you want to view.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If an IP address is not specified with this command, a list of all ARP filters is displayed.
- Enter a specific IP address to view the configuration for an individual filter.

Examples

```
-> show arp filter
 IP Addr           IP Mask             Vlan   Type       Mode
-----------------+------------------+------+----------+-------
171.11.1.1         255.255.255.255        0   target     block
172.0.0.0          255.0.0.0              0   target     block
198.0.0.0          255.0.0.0              0   sender     block
198.172.16.1       255.255.255.255      200   target     allow

-> show arp filter 198.172.16.1
 IP Addr           IP Mask             Vlan   Type       Mode
-----------------+------------------+------+----------+-------
198.0.0.0          255.0.0.0              0   sender     block
198.172.16.1       255.255.255.255      200   target     allow
```

output definitions

IP Addr	The ARP packet IP address to which the filter is applied.
IP Mask	The IP mask that specifies which part of the IP address to which the filter is applied.
Vlan	A VLAN ID. The filter is applied only to ARP packets received on ports associated with this VLAN.
Type	Indicates which IP address in the ARP packet (**sender** or **target**) is used to identify if a filter exists for that address.
Mode	Indicates whether to **block** or **allow** a switch response to an ARP packet that matches the filter.

Release History

Release 7.1.1; command introduced

Related Commands

arp filter	Adds a permanent entry to the ARP table.
clear arp filter	Deletes all dynamic entries from the ARP table.

MIB Objects

```
alaIpArpFilterTable
   alaIpArpFilterIpAddr
   alaIpArpFilterIpMask
   alaIpArpFilterVlan
   alaIpArpFilterMode
   alaIpArpFilterType
```

show icmp control

Allows the viewing of the ICMP control settings.

show icmp control

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to view the status of the various ICMP messages. It is also useful to determine the type and code of the less common ICMP messages.

Examples

```
-> show icmp control
  Name                                 Type   Code   Status    min-pkt-gap(us)
--------------------------------------+------+------+---------+-----------------
  echo reply                             0      0   enabled             0
  network unreachable                    3      0   enabled             0
  host unreachable                       3      1   enabled             0
  protocal unreachable                   3      2   enabled             0
  port unreachable                       3      3   enabled             0
  frag needed but DF bit set             3      4   enabled             0
  source route failed                    3      5   enabled             0
  destination network unknown            3      6   enabled             0
  destination host unknown               3      7   enabled             0
  source host isolated                   3      8   enabled             0
  dest network admin prohibited          3      9   enabled             0
  host admin prohibited by filter        3     10   enabled             0
  network unreachable for TOS            3     11   enabled             0
  host unreachable for TOS               3     12   enabled             0
  source quench                          4      0   enabled             0
  redirect for network                   5      0   enabled             0
  redirect for host                      5      1   enabled             0
  redirect for TOS and network           5      2   enabled             0
  redirect for TOS and host              5      3   enabled             0
  echo request                           8      0   enabled             0
  router advertisement                   9      0   enabled             0
  router solicitation                   10      0   enabled             0
  time exceeded during transmit         11      0   enabled             0
  time exceeded during reassembly       11      1   enabled             0
  ip header bad                         12      0   enabled             0
  required option missing               12      1   enabled             0
  timestamp request                     13      0   enabled             0
```

```
timestamp reply                    14      0   enabled          0
information request(obsolete)      15      0   enabled          0
information reply(obsolete)        16      0   enabled          0
address mask request               17      0   enabled          0
address mask reply                 18      0   enabled          0
```

output definitions

Name	The name of the ICMP message.
Type	The ICMP message type. This along with the ICMP code specifies the ICMP message.
Code	The ICMP message code. This along with the ICMP type specifies the ICMP message.
Status	Whether this message is **Enabled** or **Disabled**.
min-pkt-gap	The minimum packet gap, in microseconds, for this ICMP message. The minimum packet gap is the amount of time that must pass between ICMP messages of like types.

Release History

Release 7.1.1; command introduced

Related Commands

icmp type	Enables or disables a specific type of ICMP message, and sets the minimum packet gap.
icmp unreachable	Enables or disables ICMP messages pertaining to unreachable destinations, and sets the minimum packet gap.
icmp echo	Enables or disables ICMP echo messages, and sets the minimum packet gap.
icmp timestamp	Enables or disables ICMP timestamp messages, and sets the minimum packet gap.
icmp addr-mask	Enables or disables ICMP address mask messages, and sets the minimum packet gap.
icmp messages	Enables or disables all ICMP messages.

MIB Objects

N/A

show icmp statistics

Displays Internet Control Message Protocol (ICMP) statistics and errors. ICMP is a network layer protocol within the IP protocol suite that provides message packets to report errors and other IP packet processing information back to the source. ICMP generates several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages.

show icmp [statistics]

Syntax Definitions

statistics	Optional syntax.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the ICMP Table to monitor and troubleshoot the switch.

Examples

```
-> show icmp
Messages                  Received    Sent
--------------------------+-----------+------------
  Total                         2105        2105
  Error                            0           0
  Destination unreachable          0           0
  Time exceeded                    0           0
  Parameter problem                0           0
  Source quench                    0           0
  Redirect                         0           0
  Echo request                  2105           0
  Echo reply                       0        2105
  Time stamp request               0           0
  Time stamp reply                 0           0
  Address mask request             0           0
  Address mask reply               0           0
```

output definitions

Total	Total number of ICMP messages the switch received or attempted to send. This counter also includes all the messages that were counted as errors.
Error	Number of ICMP messages the switch sent/received but was unable to process because of ICMP-specific errors (for example, bad ICMP checksums, bad length).

output definitions (continued)

Destination unreachable	Number of “destination unreachable” messages that were sent/received by the switch.
Time exceeded	Number of “time exceeded” messages that were sent/received by the switch. These messages occur when a packet is dropped because the TTL counter reaches zero. When a large number of these messages occur, it is a symptom that packets are looping, that congestion is severe, or that the TTL counter value is set too low. These messages also occur when all the fragments trying to be reassembled do not arrive before the reassembly timer expires.
Parameter problem	Number of messages sent/received which indicate that an illegal value has been detected in a header field. These messages can indicate a problem in the sending IP software of the host or gateway.
Source quench	Number of messages sent/received that tell a host that it is sending too many packets. A host must attempt to reduce its transmissions upon receiving these messages.
Redirect	Number of ICMP redirect messages sent/received by the switch.
Echo request	Number of ICMP echo messages sent/received by the switch to see if a destination is active and unreachable.
Echo reply	Number of echo reply messages received by the switch.
Time stamp request	Number of time stamp request messages sent/received by the switch.
Time stamp reply	Number of time stamp reply messages sent/received by the switch.
Address mask request	Number of address mask request messages that were sent/received by the switch in an attempt to determine the subnet mask for the network.
Address mask reply	Number of address mask reply messages that were sent/received by the switch.

Release History

Release 7.1.1; command introduced

Related Commands

show udp statistics	Displays UDP errors and statistics.

MIB Objects

N/A

show tcp statistics

Displays TCP statistics.

show tcp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show tcp statistics
Total segments received =   235080,
Error segments received =        0,
Total segments sent     =   363218,
Segments retransmitted  =       38,
Reset segments sent     =       97,
Connections initiated   =    57185,
Connections accepted    =      412,
Connections established =        1,
Attempt fails           =    24393,
Established resets      =      221
```

output definitions

Total segments received	Total number of segments received, including the segments received in the error. This count includes segments received on currently established connections.
Error segments received	Total number of segments received in error (for example, bad TCP checksums).
Total segments sent	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Segments retransmitted	Number of TCP segments transmitted containing one or more previously transmitted octets.
Reset segments sent	Number of TCP segments containing the reset flag.
Connections initiated	Number of connections attempted.
Connections accepted	Number of connections allowed.
Connections established	Number of successful connections.

output definitions (continued)

Attempt fails	Number of times attempted TCP connections have failed.
Established resets	Number of times TCP connections have been reset from the "Established" or "Close Wait" state to the “Closed” state.

Release History

Release 7.1.1; command introduced

Related Commands

show icmp statistics	Displays ICMP statistics and errors.
show tcp ports	Displays the TCP connection table.

MIB Objects

N/A

show tcp ports

Displays the TCP connection table.

show tcp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this table to check the current available TCP connections.

Examples

```
-> show tcp ports
Local Address     Local Port   Remote Address    Remote Port    State
------------------+------------+-----------------+--------------+-------------
  0.0.0.0                  21   0.0.0.0                     0    LISTEN
  0.0.0.0                  23   0.0.0.0                     0    LISTEN
  0.0.0.0                  80   0.0.0.0                     0    LISTEN
  0.0.0.0                 260   0.0.0.0                     0    LISTEN
  0.0.0.0                 261   0.0.0.0                     0    LISTEN
  0.0.0.0                 443   0.0.0.0                     0    LISTEN
  0.0.0.0                6778   0.0.0.0                     0    LISTEN
  10.255.11.223            23   128.251.16.224           1867    ESTABLISHED
  10.255.11.223          2509   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2510   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2513   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2514   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2517   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2518   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2521   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2522   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2525   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2526   10.255.11.25              389    TIME-WAIT
  10.255.11.223          2529   10.255.11.33              389    TIME-WAIT
  10.255.11.223          2530   10.255.11.25              389    TIME-WAIT
```

output definitions

Local Address	Local IP address for this TCP connection. If a connection is in the LISTEN state it accepts connections for any IP interface associated with the node. The IP address 0.0.0.0 is used.
Local Port	Local port number for this TCP connection. The range is 0–65535.

output definitions (continued)

Remote Address	Remote IP address for this TCP connection.
Remote Port	Remote port number for this TCP connection. The range is 0–65535.
State	State of the TCP connection, as defined in RFC 793. A connection progresses through a series of states during its lifetime: • Listen—Waiting for a connection request from any remote TCP and port. • Syn Sent—Waiting for a matching connection request after having sent a connection request. • Syn Received—Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • Established—Open connection. Data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • Fin Wait 1—Waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent. • Fin Wait 2—Waiting for a connection termination request from the remote TCP. • Close Wait—Waiting for a connection termination request from the local user. • Closing—Waiting for a connection termination request acknowledgment from the remote TCP. • Last Ack—Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request). • Time Wait—Waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request. • Closed—No connection state.

Release History

Release 7.1.1; command introduced

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.
show tcp statistics	Displays TCP statistics.

MIB Objects

N/A

show ip tcp half-open-timeout

Displays the timeout value configured for half-open TCP sessions.

show ip tcp half-open-timeout

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip tcp half-open-timeout
Tcp Half-Open Timeout(Seconds): 15.
```

Release History

Release 8.4.1; command introduced

Related Commands

ip tcp half-open-timeout	Configures the timeout periods for dropping half-open TCP connections.

MIB Objects

```
systemServicesTcpHalfOpenTimeout
```

show udp statistics

Displays UDP errors and statistics.

show udp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command displays cumulative statistics since the last time the switch was powered on or since the last reset of the switch.

Examples

```
-> show udp statistics
Total datagrams received   =   214937,
Error datagrams received   =        0,
No port datagrams received =    32891,
Total datagrams sent       =   211884
```

output definitions

Total datagrams received	Total number of UDP datagrams delivered to UDP applications.
Error datagrams received	Number of UDP datagrams that could not be delivered for any reason.
No port datagrams received	Number of UDP datagrams that could not be delivered for reasons other than lack of application at the destination.
Total datagrams sent	Total number of UDP datagrams sent from this switch.

Release History

Release 7.1.1; command introduced

Related Commands

show udp ports	Displays the UDP Listener table.

MIB Objects

N/A

show udp ports

Displays the UDP Listener table. The table shows the local IP addresses and the local port number for each UDP listener.

show udp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- An IP address of zero (0.0.0.0) indicates that it is listening on all interfaces.
- This table contains information about the UDP end-points on which a local application is currently accepting datagrams.

Examples

```
-> show udp port
Local Address     Local Port
------------------+--------------
  0.0.0.0                  67
  0.0.0.0                 161
  0.0.0.0                 520
```

output definitions

Local Address	Local IP address for this UDP connection.
Local Port	Local port number for this UDP connection.

Release History

Release 7.1.1; command introduced

Related Commands

show udp statistics	Displays UDP errors and statistics.

MIB Objects

N/A

show ip dos config

Displays the DoS scan configuration for the switch.

show ip dos config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command allows the user to view the configuration parameters of the DoS scan. The scan keeps a record of the penalties incurred by certain types of packets on TCP and UDP ports. When the set penalty threshold is reached, it is assumed a DoS attack is in progress, and a trap is generated to inform the system administrator.

Examples

```
-> show ip dos config

   Dos type                                    Status
-------------------------------------------+-----------------
   port scan                                   ENABLED
   ping of death                               ENABLED
   loopback-src                                ENABLED
   invalid-ip                                  ENABLED
   invalid-multicast                           ENABLED
   unicast dest-ip/multicast-mac               ENABLED
   ping overload                               DISABLED
   arp flood                                   ENABLED
   arp poison

DoS trap generation                            =  ENABLED,
DoS port scan threshold                        =  1000,
DoS port scan decay                            =  2,
DoS port scan close port penalty               =  10,
DoS port scan TCP open port penalty            =  0,
DoS port scan UDP open port penalty            =  0,
Dos MAximum Ping Rate                          =  100
Dos Maximum ARP Request Rate                   =  500
```

output definitions

DoS Type	The type of DoS attack.
Status	Whether or not detection for this type of DoS attack is enabled. Configured through the **ip dos type** command.
DoS trap generation	Displays the status of DoS trap generation. It is either **ENABLED** or **DISABLED**. This is set using the **ip dos trap** command.
DoS port scan threshold	The penalty threshold setting. When enough packets have increased the penalty number to this setting, a trap is generated to warn the administrator that a DoS attack is in progress. This is set using the **ip dos scan threshold** command.
DoS port scan decay	The decay value for the switch. The penalty value of the switch is decreased by this number every minute. This is set using the **ip dos scan decay** command.
DoS port scan close port penalty	The penalty value for packets received on closed UDP and TCP ports. The penalty number for the switch is increased by this amount every time a packet is received on a closed UDP or TCP port. This is set using the **ip dos scan close-port-penalty** command.
DoS port scan TCP open port penalty	The penalty value for packets received on open TCP ports. The penalty number for the switch is increased by this amount every time a packet is received on an open TCP port. This is set using the **ip dos scan tcp open-port-penalty** command.
DoS port scan UDP open port penalty	The penalty value for packets received on open UDP ports. The penalty number for the switch is increased by this amount every time a packet is received on an open UDP port. This is set using the **ip dos scan udp open-port-penalty** command.

Release History

Release 7.1.1; command introduced

Related Commands

show ip dos statistics	Displays the statistics for detected DoS attacks on the switch.

MIB Objects

```
alaDosTable
   alaDoSType
   alaDoSStatus
alaDoSConfig
   alaDoSPortScanClosePortPenalty
   alaDoSPortScanUdpOpenPortPenalty
   alaDoSPortScanTotalPenalty
   alaDoSPortScanThreshold
   alaDoSPortScanDecay
   alaDoSTrapCntl
   alaDoSARPRate
   alaDoSPingRate
```

show ip dos statistics

Displays the statistics for detected DoS attacks on the switch.

show ip dos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command displays the number of attacks the switch has detected for several types of DoS attacks.
- If an attack is detected and reported, it does not necessarily mean that an attack occurred. The switch assumes a DoS attack is underway anytime the penalty threshold is exceeded. It is possible for this threshold to be exceeded when no attack is in progress.
- Statistics for the “unicast dest-ip/multicast-mac” DoS type are not reported for the multicast MAC address attack. In this case, the packet is dropped at a lower level so IP never sees the attack. IP only collects and reports statistics for IP attacks.

Examples

```
-> show ip dos statistics

  DoS type                              Attacks detected
----------------------------------+-------------------------
  port scan                                            0
  ping of death                                        0
  land                                                 0
  loopback-src                                         0
  invalid-ip                                           0
  invalid-multicast                                    0
  unicast dest-ip/multicast-mac                       52
  ping overload                                        0
  arp flood                                            0
  arp poison                                           0
```

output definitions

DoS type	The type of DoS attack.
Attacks detected	The number of attacks detected for each DoS type.

Release History

Release 7.1.1; command introduced

Related Commands

ip dos type	Enables or disables detection for a specific type of DoS attack.
show ip dos config	Displays the DoS scan configuration for the switch.

MIB Objects

```
alaDoSTable
   alaDoSType
   alaDoSDetected
```

show vrf

Displays the Multiple VRF instance configuration for the switch.

show vrf [*vrf_name* | **default]**

Syntax Definitions

vrf_name	The name of an existing VRF instance.
default	Selects the default VRF instance.

Defaults

By default, a list of all VRF instances is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *vrf_name* parameter to display route-map resource information for a specific VRF instance.
- Use the **default** parameter to display route-map resource information for the default VRF instance.
- The type of profile (low or max) assigned to a VRF determines the routing capabilities and the amount of route-map resources available for that specific VRF instance.

Examples

```
-> show vrf
 Virtual Routers     Profile Protocols
--------------------+-------+------------------
default              default BGP PIM VRRP
customer1            max     RIP OSPF
customer2            max     RIP OSPF
customer3            low

Total Number of Virtual Routers: 4
```

output definitions

Virtual Routers	The name of the VRF instance.
Profile	The type of profile applied to this instance (**low** or **max**).
Protocols	The protocols loaded within the context of this instance.

```
-> show vrf customer1
Legend:          in use/max
route-maps       :    3/30,
sequences        :    5/60,
tlvs             :    8/100,
access-lists     :    0/20,
address blocks   :    0/40,
match interfaces :    3/100
```

```
-> show vrf customer3
Legend:          in use/max
route-maps       :    0/10,
sequences        :    0/20,
tlvs             :    0/20,
access-lists     :    0/10,
address blocks   :    0/10,
match interfaces :    0/10

-> show vrf default
Legend:          in use/max
route-maps       :    0/200,
sequences        :    0/400,
tlvs             :    0/1000,
access-lists     :    0/200,
address blocks   :    0/500,
match interfaces :    0/2000
```

output definitions

route-maps	The number of route maps used and the maximum allowed.
sequences	The number of route map sequences used and the maximum allowed.
tlvs	The number of TLV blocks used and the maximum allowed. The TLV blocks contain the route-map match and set clauses.
access-lists	The number of route-map access lists used and the maximum allowed.
address blocks	The number of address blocks used and the maximum allowed. The address blocks hold access list addresses.
match interfaces	The number of route-map interfaces used in match clauses and the maximum allowed.

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; **Profile** field added, option to display route-map resources for a specific VRF instance.

Related Commands

vrf	Configures a Multiple VRF instance for the switch.
show vrf-profiles	Displays a summary of VRF profile usage and route map resources.
show ip protocols	Displays switch routing protocol information and status.

MIB Objects

alaVrConfigTable

- alaVrConfigIndex
- alaVrConfigRipStatus
- alaVrConfigOspfStatus
- alaVrConfigIsisStatus
- alaVrConfigBgpStatus
- alaVrConfigPimStatus
- alaVrConfigDvmrpStatus
- alaVrConfigRipngStatus
- alaVrConfigOspf3Status
- alaVrConfigMplsLdpStatus
- alaVrConfigVrrpStatus

alaVirutalRouterNameTable

- alaVirtualRouterName
- alaVirtualRouterNameIndex
- alaVirtualRouterNameRowStatus
- alaVirtualRouterProfile
- alaVirtualRouterMaxRouteMaps
- alaVirtualRouterMaxSequences
- alaVirtualRouterMaxTlvs
- alaVirtualRouterMaxAccessLists
- alaVirtualRouterMaxAddressBlocks
- alaVirtualRouterMaxMatchInterfaces

show vrf-profiles

Displays the current VRF profile usage and the maximum route-map resources allowed for each profile type (default, low, and max).

show vrf-profiles

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command also provides an estimate of the number of low profile VRFs that can be created.

Examples

```
-> show vrf-profiles
EST: Estimated number of low profile VRFs that can be created
RM:  Maximum route-maps
SEQ: Maximum sequences
TLV: Maximum TLVs (used to hold match and set clauses)
AL:  Maximum access-lists
AB:  Maximum address blocks (used to hold addresses)
ITF: Maximum route-map interfaces used in match clauses

Profile          Inuse EST  RM   SEQ  TLV  AL   AB   ITF
---------------+-----+----+----+----+----+----+----+----
default              1    -  200  400 1000  200  500 2000
low                  2  329   10   20   20   10   10   10
max                  3    -   30   60  100   20   40  100
```

Release History

Release 7.3.2; command was introduced.

Related Commands

vrf	Configures and selects a VRF instance on the switch.
show vrf	Displays the VRF configuration for the switch.

MIB Objects

```
alaVirtualRouterProfileTable
   alaVirtualRouterProfileName
   alaVirtualRouterProfileMaxRouteMaps
   alaVirtualRouterProfileMaxSequences
   alaVirtualRouterProfileMaxTlvs
   alaVirtualRouterProfileMaxAccessLists
   alaVirtualRouterProfileMaxAddressBlocks
   alaVirtualRouterProfileMaxMatchInterfaces
```

20 IPv6 Commands

This chapter details Internet Protocol Version 6 (IPv6) commands for the switch. IPv6 (documented in RFC 2460) is designed as a successor to IPv4. The changes from IPv4 to IPv6 fall primarily into the following categories:

Expanded Routing and Addressing Capabilities - IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy and a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses.

Header Format Simplification - Some IPv4 header fields were dropped or made optional, to reduce the common-case processing cost of packet handling and to keep the bandwidth cost of the IPv6 header as low as possible despite the increased size of the addresses. Even though the IPv6 addresses are four times longer than the IPv4 addresses, the IPv6 header is only twice the size of the IPv4 header.

Anycast Addressing - A new type of address called a "anycast address" is defined, to identify sets of nodes where a packet sent to an anycast address is delivered to one of the nodes. The use of anycast addresses in the IPv6 source route allows nodes to control the path on which their traffic flows.

Improved Support for Options - Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

Authentication and Privacy Capabilities - IPv6 includes the definition of extensions which provide support for authentication, data integrity, and confidentiality. This is included as a basic element of IPv6 and will be included in all implementations.

MIB information for the IPv6 and RIPng commands is as follows:

Filename: IPV6-MIB.mib
Module: Ipv6MIB

Filename: ALCATEL-IND1-IPV6-MIB.mib
Module: alcatelIND1IPv6MIB

Filename: ALCATEL-IND1-IPRMV6-MIB.mib
Module: alcatelIND1IPRMV6MIB

A summary of the IPv6 commands is listed here:

IPv6	**ipv6 interface** **ipv6 interface rtr-port** **ipv6 interface tunnel source destination** **ipv6 address** **ipv6 address global-id** **ipv6 address local-unicast** **ipv6 dad-check** **ipv6 hop-limit** **ipv6 pmtu-lifetime** **ipv6 neighbor stale-lifetime** **ipv6 neighbor** **ipv6 neighbor limit** **ipv6 neighbor vrf-limit** **ipv6 ra-filter** **ipv6 ra-filter trusted** **ipv6 prefix** **ipv6 static-route** **ipv6 static-route all bfd-state** **ipv6 static-route bfd-state** **ipv6 route-pref** **ipv6 virtual-source-mac** **ipv6 echo** **ipv6 icmp rate-limit** **ping6** **traceroute6** **modify boot parameters** **show ipv6 icmp statistics** **show ipv6 interface** **show ipv6 emp-interface** **show ipv6 emp-routes** **show ipv6 pmtu table** **show ipv6 ra-filter** **show ipv6 neighbors** **clear ipv6 neighbors** **show ipv6 prefixes** **show ipv6 routes** **show ipv6 route-pref** **show ipv6 router database** **show ipv6 tcp listeners** **show ipv6 tcp connections** **show ipv6 tunnel configured** **show ipv6 tunnel 6to4** **show ipv6 information**
IPv6 Route Map Redistribution	**ipv6 redist** **ipv6 access-list** **ipv6 access-list address** **show ipv6 redist** **show ipv6 access-list**
Route Leak	**ipv6 export** **ipv6 import** **show ipv6 export** **show ipv6 import** **show ipv6 global-route-table**

ipv6 interface

Configures an IPv6 VLAN, IPv6 tunnel, or Loopback0 interface.

ipv6 interface *if_name* **[vlan** *vlan_id* **| | service** *service_id* **| tunnel {***tunnel_id* **| 6to4} | loopback0] admin-state [enable | disable]**
[base-reachable-time *time***]**
[ra-send {yes | no}]
[ra-max-interval *interval***]**
[ra-managed-config-flag {true | false}]
[ra-other-config-flag {true | false}]
[ra-reachable-time *time***]**
[ra-retrans-timer *time***]**
[ra-default-lifetime *time* **| no ra-default-lifetime]**
[ra-min-interval *interval* **| no ra-min-interval]**
[ra-clock-skew *time***]**
[ra-preference {medium| low | high}]
[ra-send-mtu] {yes | no}
[mtu *size***]**
[retrans-timer *time***]**
[dad-transmits *count***]**
[ra-hop-limit *count***]**
[[no] local-proxy-nd]
[neighbor-limit *count* **| no neighbor-limit]**
[retrans-backoff *backoff***]**
[retrans-max *max***]**

no ipv6 interface *if_name*

Syntax Definitions

if_name	IPv6 interface name.
vlan_id	VLAN ID number to identify a VLAN interface.
service_id	An existing Shortest Path Bridging (SPB) service ID number (1–32767) to identify a service interface. *This parameter is supported only on the OmniSwitch 9900.*
tunnel_id	Tunnel ID number to identify a configured tunnel interface (*not supported on the OmniSwitch 6465 or the OmniSwitch 6560*).
6to4	Identifies the 6to4 tunnel interface (*not supported on the OmniSwitch 6465 or the OmniSwitch 6560*).
loopback0	Identifies a Loopback0 interface.
enable	Administratively enable the interface.
disable	Administratively disable the interface.
base-reachable-time *time*	Base value used to compute the reachable time for neighbors reached through this interface.
ra-send {yes | no}	Specifies whether the router advertisements are sent on this interface.

ra-max-interval *interval*	Maximum time, in seconds, allowed between the transmission of unsolicited multicast router advertisements in this interface. The range is 4–1,800.
ra-managed-config-flag {true | false}	Value to be placed in the managed address configuration flag field in router advertisements sent on this interface.
ra-other-config-flag {true | false}	Value to be placed in the other stateful configuration flag in router advertisements sent on this interface.
ra-reachable-time *time*	Value, in milliseconds, to be placed in the reachable time field in router advertisements sent on this interface. The range is 0–3,600,000. The special value of zero indicates that this time is unspecified by the router.
ra-retrans-timer *time*	Value, in milliseconds, to be placed in the retransmit timer field in router advertisements sent on this interface. The value zero indicates that the time is unspecified by the router.
ra-default-lifetime *time*	Value, in seconds, to be placed in the router lifetime field in router advertisements sent on this interface. The time must be zero or between the value of **ra-max-interval** and 9,000 seconds. A value of zero indicates that the router is not to be used as a default router. The **no ra-default-lifetime** option will calculate the value using the formula (3 * ra-max-interval).
ra-min-interval *interval*	Value, in seconds, allowed between the transmission of unsolicited multicast router advertisements on this interface. The interval must be a minimum of 3 and not more than.75 times the value of ra-max-interval.The **no ra-min-interval** option will calculate the value using the formula (.33 * ra-max-interval).
ra-clock-skew *time*	Value, in seconds. The router advertisement clock skew allows the link propagation delays and poorly synchronized clocks on routers participating in router discover over this interface. The timer differences that fall within the clock skew value are treated as valid times.
ra-preference	Specify the router preference.
ra-send-mtu {yes | no}	Specifies whether the MTU option is included in the router advertisements sent on the interface.
mtu *size*	The maximum transmission unit for a tunnel interface. Use the **vlan** command's mtu-ip to set for a VLAN.
retrans-timer *time*	The amount of time, in milliseconds, between retransmission of a neighbor solicitation during neighbor discovery.
dad-transmits *count*	The number of neighbor solicitations to send during Duplicate Address Detection.
ra-hop-limit *count*	The value placed in the current hop limit field of router advertisements sent on this interface.
[no] local-proxy-nd	Enable or disable Local Proxy Neighbor Discovery (LPND) on the interface. The default value is **no**. *LPND can only be enabled on IPv6 VLAN interfaces and is not supported on the OmniSwitch 6465 or the OmniSwitch 6560.*

neighbor-limit *count*	Sets the neighbor cache limit for the interface.The range for this value is platform dependent: • 16–64 on the OmniSwitch 6465. • 16–128 on the OmniSwitch 6560. • 10–32000 on all other supported OmniSwitch platforms. If this value is not set, then no limit is enforced.
no neighbor-limit	Sets the neighbor cache limit back to the default value (64 for OmniSwitch 6465, 128 for OmniSwitch 6560, and no limit is enforced for all other supported OmniSwitch platforms).
retrans-backoff *backoff*	Sets the Neighbor Unreachability Detection (NUD) exponential back-off base value. The configurable values are 1, 2 or 3. The default value is 1. This allows the exponentially increase of the interval between retransmissions of the Neighbor Solicitation (NS), providing a longer interval over which the neighbor can respond.
retrans-max *max*	Sets the maximum number of neighbor solicitations to be sent during ND and NUD. The range is from 1 to 10 with a default value of 3. This allows the number of neighbor solicitations sent for neighbor discovery to be increased.

Defaults

parameter	default
base-reachable-time	360
ra-send	yes
ra-max-interval	600
ra-managed-config-flag	false
ra-other-config-flag	false
ra-reachable-time	0
ra-retrans-timer	0
ra-default-lifetime	calculated
ra-min-interval	calculated
ra-clock-skew	600
ra-preference	Medium
ra-send-mtu	no
retrans-timer	1000
dad-transmits	1
ra-hop-limit	64
local-proxy-nd	no
retrans-backoff	1
retrans-max	3

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete an interface.
- When you create an IPv6 interface, it is enabled by default.
- All IPv6 VLAN, service, and tunnel interfaces must have a unique name.
- When creating an IPv6 interface for a VLAN, service, or a configured tunnel, specifying a VLAN ID, service ID, or a Tunnel ID is required. When modifying or deleting an interface, you do not need to specify one of these options unless the name assigned to the interface is being changed. If it is present with a different value from when the interface was created, the command will be in error.
- Specify the **service** parameter to create a service-based interface that is used to provide in-line routing for IPv6 over SPB. When creating an IPv6 interface for an SPB service, consider the following:
  - The SPB service ID specified must already exist in the switch configuration.
  - VLAN translation is automatically enabled when a service is assigned to an IPv6 interface regardless of whether or not VLAN translation is enabled for the service; the VLAN translation status is no longer configurable as long as the service is bound to an IPv6 interface.
  - The same SPB service ID can be assigned to an IPv4 and an IPv6 interface as long as both interface types are in the same VRF instance.
  - See the “IP over SPBM” section in the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information.
- A default 6to4 tunnel named “tunnel_6to4” is automatically created in the default VRF instance. The tunnel status and configuration can be changed, but the tunnel itself cannot be deleted.
- The 6to4 tunnel interface and the Loopback0 interface do not send router advertisements (**ra-send** is always set to **no**).
- Before a 6to4 tunnel or Loopback0 interface can be enabled, at least one address must be assigned to the interface.
- To enable IPv6 routing you must first create a VLAN, then create an IPv6 interface on the VLAN. See Chapter 5, “VLAN Management Commands,” for information on creating VLANs.
- To route IPv6 traffic over an IPv4 network, you must create an IPv6 tunnel using the **ipv6 interface** command.
- Use the **no** option to disable the Local Proxy Neighbor Discovery on the interface.
- Consistency checks are performed between the configured RA parameters and those present in received RAs. In the case of a discrepancy between the value in a received RA and the value configured on the switch, an informational message will be written to the SWLog log file. The messages are not logged on the console.
- The **ra-managed-config-flag** and **ra-other-config flag** parameters specify the values to be present in RAs sent by the switch when the DHCPv6 server is disabled. If the DHCPv6 server is enabled, the M and O flags in RAs sent by the switch will always be true.

Examples

```
-> ipv6 interface Test vlan 1
-> ipv6 interface Test_Tunnel tunnel 2
-> ipv6 interface Mgmt_intf loopback0
-> ipv6 interface vpn1 service 10
-> service 10 vlan-xlation disable
```

```
ERROR: Modify vlan translation currently not allowed for service (10)
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **loopback0** parameter added.

Related Commands

show ipv6 interface	Displays IPv6 Interface Table.
show ipv6 tunnel configured	Displays IPv6 Configured Tunnel.
show ipv6 tunnel 6to4	Displays IPv6 6to4 tunnel information.
show ipv6 information	Displays IPv6 information.

MIB Objects

```
IPv6Ifindex
alaIPv6InterfaceTable
   alaIPv6InterfaceName
   alaIPv6InterfaceMtu
   alaIPv6InterfaceSendRouterAdvertisements
   alaIPv6InterfaceMaxRtrAdvInterval
   alaIPv6InterfaceAdvManagedFlag
   alaIPv6InterfaceAdvOtherConfigFlag
   alaIPv6InterfaceAdvRetransTimer
   alaIPv6InterfaceAdvDefaultLifetime
   alaIPv6InterfaceAdminStatus
   alaIPv6InterfaceAdvReachableTime
   alaIPv6InterfaceBaseReachableTime
   alaIPv6InterfaceAdvSendMtu
   alaIPv6InterfaceLPND
   alaIPv6InterfaceNeighborLimit
   alaIPv6InterfaceRetransBackoff
   alaIPv6InterfaceRetransMax
```

ipv6 interface rtr-port

Configures an IPv6 routed-port interface by associating an IPv6 interface with a port or link aggregate and a VLAN.

ipv6 interface *if_name* **rtr-port {port** *chassis/slot/port* **| linkagg** *agg_id***} {tagged | untagged} vlan** *vlan_id*

Syntax Definitions

if_name	A unique name for the IPv6 interface. Use quotes around the string if the name contains multiple words with spaces between them (for example, “ALE Marketing”). This value is case sensitive.
chassis/slot/port	The chassis, slot, and port number (1/2/1) of the physical port to bind to the IPv6 interface.
agg_id	The link aggregate ID to bind to the IP Interface.
tagged	Whether the assigned port or link aggregate is tagged for the specified VLAN.
untagged	Whether the assigned port or link aggregate is untagged for the specified VLAN.
vlan_id	An unused VLAN ID to which this IPv6 interface is associated.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- In a single step, this command creates the specified VLAN, configures an IPv6 interface for the VLAN, and assigns a port or link aggregate (tagged or untagged) to the VLAN. The **ipv6 address** command is then used to assign and IPv6 address to the routed-port interface.
- Configuring an IPv4 and IPv6 routed-port interface for the same VLAN ID is supported if the following conditions are met:
  - The VLAN ID, port, and the tagged/untagged port status for both interfaces is the same (for example, IPv4 and IPv6 routed interfaces are both bound to VLAN 850 with port 1/1/2 tagged).
  - Both interfaces are configured in the same VRF instance.
- Make sure the specified VLAN ID does not already exist in the switch configuration or is only used as a routed-port VLAN for an IPv4 interface. This VLAN will serve as a routing-only VLAN with a single port or link aggregate (Layer 2 functionality is not supported).
- Make sure the specified port or link aggregate is not already assigned to a VLAN that is not a routed-port VLAN. However, the port or link aggregate can be assigned to other routed-port VLANs.

- Attempting to add more ports or link aggregates to the routed-port VLAN or attempting to delete the VLAN is not allowed. The VLAN can only be removed by deleting the associated IPv6 and, if configured, the associated IPv4 interface.
- The same VLAN cannot be used for both a routed-port interface and a non-routed port interface.
- Once configured, an IPv6 routed port interface is operationally equivalent to an IPv6 VLAN interface. Routing protocols and other switch features that use IPv6 are configured and operate on an IPv6 routed port interface in the same manner as on a regular IPv6 interface.

Examples

```
-> ipv6 interface rp-vlan30 rtr-port port 1/1/1 tagged vlan 30
-> ipv6 interface rp-vlan40 rtr-port port 1/1/2 untagged vlan 40
-> ipv6 interface rp-vlan50 rtr-port linkagg 6 tagged vlan 50
-> ipv6 interface rp-vlan60 rtr-port linkagg 7 untagged vlan 60
-> ipv6 interface rp-vlan60 rtr-port port 1/1/3 untagged vlan 60
ERROR: Routed port interface rp-vlan60 VLAN and/or port configuration cannot be
changed
-> no ipv6 interface rp-vlan60

-> vlan 70
-> ipv6 interface rp-vlan70 rtr-port port 1/1/15 untagged vlan 70
ERROR: VLAN 70 already exists

-> ip interface rpv4-port rtr-port port 1/1/2 tagged vlan 850
-> ipv6 interface rpv6-port rtr-port port 1/1/2 tagged vlan 850

-> no ipv6 interface rpv6-port
-> ipv6 interface rpv6-port rtr-port port 1/1/2 untagged vlan 850
ERROR: Configuration conflict with IPv4 routed port interface rp-port
```

Release History

Release 8.6R2; command introduced

Related Commands

show ipv6 interface	Displays the status and configuration of IPv6 interfaces.

MIB Objects

```
alaIPv6InterfaceTable
   alaIPv6InterfaceName
   alaIPv6InterfaceRoutedPortIfIndex
   alaIPv6InterfaceRoutedPortTag
```

ipv6 interface tunnel source destination

Configures the source and destination IPv4 addresses for a configured tunnel.

ipv6 interface *if_name* **tunnel {source** *ipv4_source* **destination** *ipv4_destination***}**

Syntax Definitions

if_name	Name assigned to the tunnel interface.
ipv4_source	Source IPv4 address for the configured tunnel.
ipv4_destination	Destination IPv4 address for the configured tunnel.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **ipv6 interface** command to create an IPv6 tunnel interface.
- A configured tunnel interface cannot be enabled until both its IPv4 source and destination addresses have been specified.

Examples

```
-> ipv6 interface Test tunnel 2 source 192.0.2.1 destination 198.51.100.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 interface	Creates an IPv6 tunnel interface.
show ipv6 tunnel configured	Displays IPv6 tunnel information.

MIB Objects

```
IPv6IfIndex
   alaIPv6ConfigTunnelv4Source
   alaIPv6ConfigTunnelv4Dest
   alaIPv6ConfigTunnelRowStatus
```

ipv6 address

Configures an IPv6 address for an IPv6 interface. There are different formats for this command depending on the address type.

ipv6 address *ipv6_address /prefix_length* **{***if_name* | **loopback}**

no ipv6 address *ipv6_address* **{***if_name* **| loopback}**

ipv6 address *ipv6_prefix* **eui-64 {***if_name* | **loopback}**

no ipv6 address *ipv6_prefix* **eui-64 {***if_name* | **loopback}**

Syntax Definitions

ipv6_address	IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask). (3..128).
eui-64	Append an EUI-64 identifier to the prefix.
if_name	Name assigned to the interface.
loopback	Configures an IPv6 address for the loopback interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete an address.
- You can assign multiple IPv6 addresses to an IPv6 interface.
- No default value for prefix length. However, the prefix for the loopback or the user-defined Loopback0 interface must always be /128.
- Make sure that only 6to4 addresses are assigned to a 6to4 tunnel interface.
- The “eui” form of the command is used to add or remove an IPv6 address for a VLAN or configured tunnel using an EUI-64 interface ID in the low order 64 bits of the address.
- When JITC mode is enabled, Site-Local addresses of range FEC0::/10 cannot be configured. This consists of all the addresses that begin with FEC, FED, FEE, and FEF. Refer to the “AAA Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide* for more information on enabling JITC mode.

Examples

```
-> ipv6 address 2001:db8:4132:86::19a/64 Test_Lab
-> ipv6 address 2002:c633:6489::35/64 Test_6to4
```

```
-> ipv6 address 2001:db8:6489::36/128 loopback
-> ipv6 interface Test_Loopback0 loopback0
-> ipv6 address 2001:db8:6489::37/128 Test_Loopback0
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1: **anycast** keyword deprecated.

Related Commands

show ipv6 interface	Displays IPv6 Interface Table.

MIB Objects

```
IPv6IfIndex
alaIPv6InterfaceAddressTable
   alaIPv6InterfaceAddress
   alaIPv6InterfaceEUI64AddressPrefixLength
   alaIPv6InterfaceEUI64AddressrowStatus
For EUI-64 Addresses:
alaIPv6InterfaceEUI64AddresssTable
   alaIPv6InterfaceEUI64Address
   alaIPv6InterfaceEUI64AddressPrefixLength
   alaIPv6InterfaceEUI64AddressRowStatus
```

ipv6 address global-id

Automatically generates or allows a new global ID to be entered.

ipv6 address global-id {generate | *globalID*}

Syntax Definitions

generate	Automatically generates the global ID.
globalID	A 5-byte global ID value specified in the form hh:hhhh:hhhh

Defaults

By default, the IPv6 global ID is set to all zeros.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Global ID needs to be automatically generated or configured explicitly.
- A 40-bit global identifier is used to make the local IPv6 address prefixes globally unique.
- The global ID will be generated the first time a local unicast address is added through the **ipv6 address local-unicast** command or when the **ipv6 address global-id** command is executed.

Examples

```
-> ipv6 address global-id generate
-> ipv6 address global-id 32:57a3:8fed
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 address local-unicast	Creates a IPv6 local unicast address using the configured global ID.
ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaIPv6GlobalID
```

ipv6 address local-unicast

Creates a IPv6 local unicast address using the configured global ID.

ipv6 address local-unicast [global-id *globalID***] [subnet-id** *subnetID***] {interface-id** *interfaceID* **| eui-64} [prefix-length** *prefixLength***] {***if_name* **| loopback}**

no ipv6 address local-unicast [global-id *globalID***] [subnet-id** *subnetID***] {interface-id** *interfaceID* **| eui-64} [prefix-length** *prefixLength***]** *{if_name* **| loopback}**

Syntax Definitions

globalID	A 5-byte global ID value specified in the form hh:hhhh:hhhh.
subnetID	A 2-byte Subnet ID specified in the form 0xhhhh. The valid range is 0x0000-0xffff or 0-65535.
interfaceID	An interface identifier specified in the form hhhh:hhhh:hhhh:hhhh.
eui-64	Automatically-generated EUI-64 value to be used for interface identfier.
prefixLength	The number of bits that are significant in the IPv6 address (mask). The valid range is 0-128; however, the default value must rarely be overridden.
if_name	The name assigned to the interface.
loopback	The loopback for the loopback interface.

Defaults

parameter	default
prefixLength	64

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the local unicast address. However, addresses are normally deleted using the **ipv6 address** command.
- If the global ID value is not explicitly specified, the default global ID set by the **ipv6 address global-id** command is used.
- If the global ID value is explicitly configured using the **ipv6 address local-unicast** command, the address' global ID will not be changed if the **ipv6 address global-id** command is executed.
- The use of a double-colon abbreviation for the interface identifier, similar to that used for full IPv6 addresses, is allowed.

Examples

```
-> ipv6 address local-unicast global-id 0073:110:255 subnet-id 23 interface-id
215:60ff:fe7a:adc0 prefix-length 64 loopback
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 address global-id	Automatically generates or allows a new global ID to be entered.
show ipv6 information	Displays IPv6 information.

MIB Objects

```
alaIPv6LocalUnicastGlobalID
alaIPv6LocalUnicastSubnetID
alaIPv6LocalUnicastInterfaceID
alaIPv6LocalUnicastEUI64
alaIPv6LocalUnicastPrefixLength
```

ipv6 dad-check

Runs a Duplicate Address Detection (DAD) check on an address that was marked as duplicated.

ipv6 dad-check *ipv6_address if_name*

Syntax Definitions

ipv6_address	IPv6 address.
if_name	Name assigned to the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The switch performs DAD check when an interface is attached and its VLAN first enters the active state. Use this command to rerun a DAD check on an address that was marked as duplicated.

Examples

```
-> ipv6 dad-check 2001:db8::1/32 Test_Lab
```

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIPv6InterfaceAddressTable
   alaIPv6InterfaceAddressDADStatus
```

ipv6 hop-limit

Configures the value placed in the hop limit field in the header of all IPv6 packets that are originated by the switch. It also configures the value placed in the hop limit field in router advertisements.

ipv6 hop-limit *value*

no ipv6 hop-limit

Syntax Definitions

value	Hop limit value. The range is 0 - 255.

Defaults

parameter	default
value	64

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to return the hop limit to its default value.
- Inputting the value 0 (zero) will result in the default (64) hop-limit.

Examples

```
-> ipv6 hop-limit 64
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 information	Displays IPv6 information.

MIB Objects

```
ipv6MibObjects
   Ipv6DefaultHopLimit
```

ipv6 pmtu-lifetime

Configures the minimum lifetime for entries in the path MTU Table.

ipv6 pmtu-lifetime *time*

Syntax Definitions

time	Minimum path MTU entry lifetime, in minutes. Valid range is 10–1440.

Defaults

parameter	default
time	10

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ipv6 pmtu-lifetime 30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pmtu table	Displays the IPv6 path MTU Table.
show ipv6 information	Displays IPv6 information.

MIB Objects

```
alaIPv6ConfigTable
   alaIPv6PMTUMinLifetime
```

ipv6 neighbor stale-lifetime

Configures the minimum lifetime for neighbors in the unconfirmed state.

ipv6 neighbor stale-lifetime *stale-lifetime*

Syntax Definitions

stale-lifetime	Minimum lifetime for neighbor entries in the stale state (5–2800).

Defaults

parameter	default
stale-lifetime	10

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ipv6 neighbor stale-lifetime 1400
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 neighbors	Displays IPv6 Neighbor Table.
show ipv6 information	Displays IPv6 information.

MIB Objects

```
IPv6IfIndex
alaIPv6NeighborTable
   alaIPv6NeighborStaleLifetime
```

ipv6 neighbor

Configures a static entry in the IPv6 Neighbor Table.

ipv6 neighbor *ipv6_address hardware_address* **{***if_name***} {port** *chassis/slot/port* | **linkagg** *agg_id*}

no ipv6 neighbor *ipv6_address* **{***if_name***}**

Syntax Definitions

ipv6_address	IPv6 address that corresponds to the hardware address.
hardware_address	MAC address in hex format (e.g., 00:00:39:59:F1:0C).
if_name	Name assigned to the interface on which the neighbor resides.
chassis	The chassis identifier.
slot/port	The slot and port number of the port used to reach the neighbor.
agg_id	The link aggregate ID number of the link aggregate used to reach the neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove an entry from IPv6 Neighbor Table.

Examples

```
-> ipv6 neighbor 4132:86::203 00:d0:c0:86:12:07 Test port 1/1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 neighbors	Displays IPv6 Neighbor Table.

MIB Objects

```
IPv6IfIndex
alaIPv6NeighborTable
   alaIPv6NeighborNetAddress
   alaIPv6NeighborPhysAddress
   alaIPv6NeighborSlot
   alaIPv6NeighborPort
   alaIPv6NeighborRowStatus
   alaIPv6NeighborStaleLifetime
```

ipv6 neighbor limit

Configures the system-wide maximum limit for the number of neighbor entries in the cache.

ipv6 neighbor limit *count*

no ipv6 neighbor limit

Syntax Definitions

count	The system-wide maximum limit for the number of neighbor entries in the cache. The valid range for this value is platform dependent: • 16–64 on the OmniSwitch 6465. • 16–128 on the OmniSwitch 6560. • 200–32000 on all other supported OmniSwitch platforms. If this value is not set, then no limit is enforced.

Defaults

By default, the maximum number of neighbor entries is set to 64 on the OmniSwitch 6465 and 128 on the OmniSwitch 6560. On all other supported OmniSwitch platforms, there is no enforced limit.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to set the limit back to the default value.

Examples

```
-> ipv6 neighbor limit 16
-> ipv6 neighbor limit 200
-> no ipv6 neighbor limit
```

Release History

Release 8.1.1; command introduced.

Related Commands

ipv6 interface	Creates an IPv6 tunnel interface.
show ipv6 information	Displays IPv6 information.

MIB Objects

```
alaIPv6NeighborTable
   alaIPv6NeighborLimit
```

ipv6 neighbor vrf-limit

Configures the maximum limit for the number of neighbor entries in a VRF's cache.

ipv6 neighbor vrf-limit *count*

no ipv6 neighbor vrf-limit

Syntax Definitions

count	The maximum limit for the number of VRF neighbor entries in the cache. The valid range for this value is platform dependent: • 16–64 on the OmniSwitch 6465. • 16–128 on the OmniSwitch 6560. • 200–32000 on all other supported OmniSwitch platforms. If this value is not set, then no limit is enforced.

Defaults

By default, the maximum number of neighbor entries is set to 64 on the OmniSwitch 6465 and 128 on the OmniSwitch 6560. On all other supported OmniSwitch platforms, there is no enforced limit.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to set the limit back to the default value.

Examples

```
-> ipv6 neighbor vrf-limit 16
-> ipv6 neighbor vrf-limit 200
-> no ipv6 neighbor vrf-limit
```

Release History

Release 8.1.1; command introduced.

Related Commands

ipv6 interface	Creates an IPv6 tunnel interface.
show ipv6 information	Displays IPv6 information.

MIB Objects

```
alaIPv6NeighborTable
   alaIPv6NeighborVRFLimit
```

ipv6 ra-filter

Configures the status of Router Advertisement (RA) filtering on IPv6 VLAN interfaces. When RA filtering is enabled on an interface, RAs received on any port or linkagg will be discarded. If one or more trusted ports or link aggregates are configured, RAs received on them will be accepted and sent on to any connected IPv6 nodes.

ipv6 ra-filter *if-name* **[admin-state {enable | disable}]**

no ipv6 ra-filter *if-name*

Syntax Definitions

if-name	Specify the name of the IPv6 VLAN interface.
enable	Enables RA filtering on the specified interface.
disable	Disables RA filtering on the specified interface.

Defaults

By default, the administrative status of RA filtering on an IPv6 VLAN interface is disabled.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900

Usage Guidelines

Use the **no** form of this command to return the RA filtering status to the default value (disabled).

Examples

```
-> ipv6 ra-filter vlan-23 admin-state enable
-> ipv6 ra-filter vlan-23 admin-state disable
-> no ipv6 ra-filter vlan-23
```

Release History

Release 8.1.1; command introduced.
Release 8.5R2; OmniSwitch 6560 support for IPv6 RA Filtering added.

Related Commands

ipv6 ra-filter trusted	Configures trusted ports or link aggregates on which RAs are accepted when RA filtering is enabled.
ipv6 interface	Creates an IPv6 interface.
show ipv6 interface	Displays IPv6 Interface Table.
show ipv6 ra-filter	Displays the RA filter configuration for an IPv6 interface.

MIB Objects

```
alaIPv6RAFilterInterfaceTable
   alaIPv6RAFilterInterfaceAdminStatus
   alaIPv6RAFilterInterfaceRowStatus
```

ipv6 ra-filter trusted

Configures trusted sources (ports or link aggregates) on which Router Advertisements (RAs) are accepted and sent on to any connected IPv6 nodes. When RA filtering is enabled on an IPv6 VLAN interface, RAs received on any port or linkagg will be discarded, except on trusted ports or link aggregates.

ipv6 ra-filter *if-name* **trusted {port** *chassis/slot/port* **| linkagg** *agg_num***}**

no ipv6 ra-filter *if-name* **trusted {port** *chassis/slot/port* **| linkagg** *agg_num***}**

Syntax Definitions

if-name	Specify the name of the IPv6 VLAN interface on which RA filtering is enabled or disabled.
chassis/slot/port	The chassis ID, slot, and port number (3/1/1) for a trusted port.
agg_num	A trusted link aggregate ID number.

Defaults

By default all ports and link aggregates are untrusted.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to return a port or linkagg to an untrusted state.
- Use the **ipv6 ra-filter** command to enable or disable the RA filtering status for an IPv6 VLAN interface.

Examples

```
-> ipv6 ra-filter vlan-23 trusted port 1/1/22
-> ipv6 ra-filter vlan-23 trusted linkagg 10
-> no ipv6 ra-filter vlan-23 trusted port 1/1/22
-> no ipv6 ra-filter vlan-23 trusted linkagg 10
```

Release History

Release 8.1.1; command introduced.
Release 8.5R2; OmniSwitch 6560 support for IPv6 RA Filtering added.

Related Commands

ipv6 ra-filter	Configures the RA filtering status for an IPv6 VLAN interface.
ipv6 interface	Creates an IPv6 tunnel interface.
show ipv6 interface	Displays IPv6 Interface Table.
show ipv6 ra-filter	Displays the RA filter configuration for an IPv6 interface.

MIB Objects

```
alaIPv6RAFilterTrustedSourceTable
   alaIPv6RAFilterTrustedSourceRowStatus
```

ipv6 prefix

Configures an IPv6 prefix on an interface. Used for configuring prefixes for router advertisements.

ipv6 prefix *ipv6_address /prefix_length if_name* **[valid-lifetime** *time***] [preferred-lifetime** *time***] [on-link-flag {true | false} [autonomous-flag {true | false}]** *if_name*

no ipv6 prefix *ipv6_address /prefix_length if_name*

Syntax Definitions

ipv6_address	IPv6 address of the interface.
/prefix_length	The number of bits that are significant in the IPv6 address (mask). (1...127).
valid-lifetime *time*	Length of time, in seconds, that this prefix will remain valid (i.e. time until deprecation). A value of 4,294,967,295 represents infinity.
preferred-lifetime *time*	Length of time, in seconds, that this prefix will remain preferred (i.e. time until deprecation). A value of 4,294,967,295 represents infinity.
on-link-flag {true | false}	On-link configuration flag. When “true” this prefix can be used for on-link determination.
autonomous-flag {true | false}	Autonomous address configuration flag. When “true”, indicates that this prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
if_name	Name assigned to the interface.

Defaults

parameter	default
valid-lifetime *time*	2,592,000
preferred-lifetime *time*	604,800
on-link-flag	true
autonomous-flag	true

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to delete a prefix.

Examples

```
-> ipv6 prefix 4132:86::/64 Test
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 prefixes	Displays IPv6 prefixes used in router advertisements.

MIB Objects

```
IPv6IfIndex
alaIPv6InterfacePrefixTable
   alaIP6vInterfacePrefix
   alaIP6vInterfacePrefixLength
   alaIP6vInterfacePrefixValidLifetime
   alaIP6vInterfacePrefixPreferredLifetime
   alaIP6vInterfacePrefixonLinkFlag
   alaIP6vInterfacePrefixAutonomousFlag
   alaIP6vInterfacePrefixRowStatus
```

ipv6 static-route

Configures an IPv6 static route. Static routes are user-defined; they carry a higher priority than routes created by dynamic routing protocols. By default, static routes carry a higher priority than dynamic routes.

ipv6 static-route *ipv6_prefix/prefix_length* **gateway {***ipv6_address* **| null} [tag** *num***] [name** *string***] [***if_name***] [emp] [metric** *metric***]**

no ipv6 static-route *ipv6_prefix/prefix_length* **gateway {***ipv6_address* **| null} [** *if_name***] [emp]**

Syntax Definitions

ipv6_prefix	IPv6 network that is the destination of this static route.
/prefix_length	The number of bits (0...128) that are significant in the iPv6 address (mask).
gateway *ipv6_address*	IPv6 address of the next hop used to reach the destination IPv6 address.
gateway null	Use this option to configure an IPv6 blackhole route.
num	Tag to be used for route.
string	Name to be used for route.
if_name	If the next hop is a link-local address, the name of the interface used to reach it.
emp	Represents the EMP interface.
metric	Metric or cost (hop count) for the static route. You can set a priority for the static route by assigning a metric value. The lower the metric value, the higher the priority. Valid range is 1–15.

Defaults

parameter	default
metric	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a static route.
- By default, static routes have a higher priority over dynamic routes; however, it can be changed using the **ipv6 route-pref** command.
- To create an IPv6 static route with gateway pointing to an EMP interface, specify the keyword **emp** for the interface name field instead of specifying the exact interface name of the EMP interface (for example, EMP-CMMA-CHAS1).
- If IPv6 address is configured on the EMP port on a VC or chassis setup, ensure to configure the IPv6 address on all the VC elements or CMM.
- Static route with default gateway towards EMP interface is not allowed.

- Use the **null** option to configure IPv6 blackhole routes. A blackhole route is used to forward unwanted traffic to a blackhole.
  - Redistribution of blackhole routes is supported. Dynamic routing protocols may advertise these routes, but the gateway associated with the route(s) will be an address on the router advertising them.
  - Leaking of blackhole routes across SPB service backbones is supported. However, blackhole routes cannot be leaked between VRFs. Blackhole routes need to be explicitly configured using the **ip static-route** command in any/all VRFs.
  - Blackhole routes are created and installed through static route commands. Dynamic Routing protocols shall not install blackhole IPv6 routes.
  - Blackhole routes shall never be part of ECMP.
  - Blackhole routes cannot be enabled for BFD support.
- Alternatively, the gateway address '::' can be used to create an IPv6 blackhole route.

Examples

```
-> ipv6 static-route 212:95:5::/64 gateway fe80::2d0:95ff:fe6a:f458 v6if-137 metric 3
```

Static route with gateway towards EMP interface:

```
-> ipv6 static-route 212:95:5::/64 gateway 2001::205 emp
or
-> ipv6 static-route 212:95:5::/64 gateway 2001::205 EMP-CMMA-CHAS1
```

Static route with default gateway towards EMP interface is not allowed.

```
-> ipv6 static-route ::/0 gateway 2001::205 EMP-CMMA-CHAS1
ERROR: Default routes with gateway on EMP port not allowed
```

Configuring a static blackhole route.

```
-> ipv6 static-route 212:95:5::/64 gateway null

-> ipv6 static-route 22::/64 gateway ::
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **tag** and **name** parameters included.
Release 8.4.1; **emp** parameter added.
Release 8.6R1; **null** keyword added.

Related Commands

modify boot parameters	This command is used to configure IPv6 EMP interface.
show ipv6 routes	Displays IPv6 Forwarding Table.
show ipv6 router database	Displays a list of all routes (static and dynamic) that exist in the IPv6 router database.
show ipv6 route-pref	Displays the IPv6 routing preference of the router.

MIB Objects

```
alaIprmv6StaticRouteTable
   alaIprmv6StaticRouteDest
   alaIprmv6StaticRoutePrefixLength
```

```
alaIprmv6StaticRouteNextHop
alaIprmV6StaticRouteTag
alaIprmV6StaticRouteName
alaIprmv6StaticRouteIfIndex
alaIprmv6StaticRouteMetric
alaIprmv6StaticRouteRowStatus
```

ipv6 static-route all bfd-state

Enables BFD for all IPv6 static routes.

ipv6 static-route all bfd-state {enable| disable}

Syntax Definitions

enable	Enables BFD for all IPv6 static routes.
disable	Disables BFD for all IPv6 static routes.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When there are static routes configured in the switch, BFD is enabled to track the gateway.
- If the route is not reachable, it will be moved to the inactive database.

Examples

```
-> ipv6 static-route all bfd-state enable
-> ipv6 static-route all bfd-state disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 static-route bfd-state	Enables BFD for a specific static route.
show ipv6 router database	Displays a list of all routes (static and dynamic) that exist in the IP router database.

MIB Objects

```
alaIprmV6Config
   alaIprmV6StaticAllBfd
```

ipv6 static-route bfd-state

Enables or disables BFD for a specific IPv6 static route.

ipv6 static-route *ipv6_prefix/pfx_length* **gateway** *ipv6_host_address* **bfd-state {enable| disable}**

Syntax Definitions

ipv6_prefix	The destination IPv6 address.
pfx_length	The prefix length for the destination IPv6 address.
ipv6_host_address	The gateway IPv6 address.
enable	Enables BFD for the IPv6 static route.
disable	Disables BFD for the IPv6 static route.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

BFD is enabled to track the gateway of static routes.

Examples

```
-> ipv6 static-route 195:35::/64 gateway fe80::2d0:95ff:fe12:f470 bfd-state enable
-> ipv6 static-route 195:35::/64 gateway fe80::2d0:95ff:fe12:f470 bfd-state disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 static-route all bfd-state	Enables BFD for all static routes.
show ipv6 router database	Displays a list of all routes (static and dynamic).

MIB Objects

```
alaIprmV6StaticRouteTable
   alaIprmV6StaticRouteDest
   alaIprmV6StaticRoutePfxLength
   alaIprmV6StaticRouteNextHop
   alaIprmV6StaticRouteIfIndex
   alaIprmV6StaticRouteBfdStatus
   alaIprmV6StaticRouteType
```

ipv6 route-pref

Configures the route preference of a router.

ipv6 route-pref {static | ospf | rip | ebgp | ibgp | isisl1 | isisl2 | import} *value*

Syntax Definitions

static	Configures the route preference of static routes.
ospf	Configures the route preference of OSPF3 routes (*OSPF3* is *not supported on the OmniSwitch 6465 or OmniSwitch 6560*).
rip	Configures the route preference of RIPng routes.
ebgp	Configures the route preference of external BGP routes (*the IPv6 version of BGP is not supported on the OmniSwitch 6465 or OmniSwitch 6560*).
ibgp	Configures the route preference of internal BGP routes (*the IPv6 version of BGP is not supported on the OmniSwitch 6465 or OmniSwitch 6560*).
isisl1	Configures the route preference of IS-IS L1 routes (*IS-IS* is *not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 9900*).
isisl2	Configures the route preference of IS-IS L2 routes (*IS-IS* is *not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 9900*).
import	Configures the route preference for the routes that are imported from another VRF instance.
value	Route preference value. The valid range is 1–255.

Defaults

parameter	default
static *value*	2
ospf *value*	110
rip *value*	120
ebgp *value*	190
ibgp *value*	200
isisl1 *value*	115
isisl1 *value*	118
import *value*	210

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Route preference of local routes cannot be changed.

Examples

```
-> ipv6 route-pref ospf 20
-> ipv6 route-pref rip 60
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R1; **import** parameter added.

Related Commands

show ipv6 route-pref	Displays the configured route preference of a router.

MIB Objects

```
alaIprmV6RtPrefTable
   alaIprmV6RtPrefEntryType
   alaIprmV6RtPrefEntryValue
```

ipv6 virtual-source-mac

Configures the source MAC to be used for packets being sent from a VRRP instance.

ipv6 virtual-source-mac {on | off}

Syntax Definitions

on	The switch will use the VRRP virtual MAC address for all packets.
off	The switch will use the physical MAC address for all packets except VRRP advertisements.

Defaults

parameter	default
virtual-source-mac	off

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to change which MAC address the switch will use as the source MAC when sending packets from a VRRP instance.
- This command has no affect on VRRP advertisements, the VRRP virtual MAC will always be used.

Examples

```
-> ipv6 virtual-source-mac on
-> ipv6 virtual-source-mac off
```

Release History

Release 7.2.1; command was introduced.

Related Commands

show ipv6 route-pref	Displays the configured route preference of a router.

MIB Objects

N/A

ipv6 echo

Configures the switch to reply or ignore echo requests in response to an echo request sent to a multicast or anycast IPv6 address. Use **no** option to ignore reply to anycast or multicast echo requests.

ipv6 echo {anycast | multicast}

no ipv6 echo {anycast | multicast}

Syntax Definitions

anycast	Ignore (when **no** option is used) or reply to anycast echo requests.
multicast	Ignore (when **no** option is used) or reply to multicast echo requests.

Defaults

By default, the switch will reply to multicast or anycast echo requests.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The switch will not ignore echo requests that it originates that are destined to one of its own anycast or multicast addresses.

Examples

```
-> ipv6 echo multicast
-> no ipv6 echo anycast
```

Release History

Release 8.4.1; command introduced.

Related Commands

show ipv6 information	Displays IPv6 information.

MIB Objects

```
alaIPv6IgnoreAnycastEchos
alaIPv6IgnoreMcastEchos
```

ipv6 icmp rate-limit

Configures the rate-limiting of ICMPv6 error messages.

ipv6 icmp rate-limit [interval *number***] [burst** *number***]**

no ipv6 icmp rate-limit

Syntax Definitions

interval *number*	The minimum interval between the ICMPv6 error messages.Valid range is 0 to 10000 in milliseconds.
burst *number*	The maximum number of ICMPv6 error messages that may be sent in a single burst regardless of the interval. Valid range is 1 to 50.

Defaults

parameter	default
interval *number*	10ms
burst *number*	10

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use **no** option to disable the ICMPv6 error message rate limiting.

Examples

```
-> ipv6 icmp rate-limit interval 100
-> ipv6 icmp rate-limit burst 20
-> no ipv6 icmp rate-limit
```

Release History

Release 8.4.1; command introduced.

Related Commands

show ipv6 information	Displays IPv6 information.

MIB Objects

```
alaIPv6IcmpRateLimitInterval
alaIPv6IcmpRateLimitBurst
```

ping6

Tests whether an IPv6 destination can be reached from the local switch. This command sends an ICMPv6 echo request to a destination and then waits for a reply. To ping a destination, enter the **ping6** command and enter either the destination's IPv6 address or hostname. The switch will ping the destination using the default frame count, packet size, and interval (6 frames, 64 bytes, and 1 second respectively). You can also customize any or all of these parameters as described below.

ping6 {*ipv6_address* | *hostname***}** [*if_name*] **[count** *count***] [size** *data_size***] [interval** *seconds***]**

Syntax Definitions

ipv6_address	The IP address of the system to ping.
hostname	DNS name of the system to ping.
if_name	If the target is a link-local address, the name of the interface used to reach it.
count	Number of packets to be transmitted.
size	Size of the data portion of the packet sent for this ping, in bytes.
seconds	Interval, in seconds, at which ping packets are transmitted.

Defaults

parameter	default
count	6
size	8
interval *seconds*	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If you change the default values, they will only apply to the current ping. The next time you use the ping command, the default values will be used unless you again enter different values.
- When the next hop address is a local link address, the name of the interface used to reach the destination must be specified.

Examples

```
-> ping6 2001:db8:302::44
-> ping6 fe80::2d0:95ff:fe6a:f458 vlanif-23
```

Release History

Release 7.1.1; command was introduced.

Related Commands

traceroute6	Finds the path taken by an IPv6 packet from the local switch to a specified destination.

MIB Objects

N/A

traceroute6

Finds the path taken by an IPv6 packet from the local switch to a specified destination. This command displays the individual hops to the destination as well as some timing information.

traceroute6 {*ipv6_address* | *hostname*} [*if_name*] **[max-hop** *hop_count***] [dest-port** *port_number***] [probe-count** *probe***] [size** *size***] [host-names** {**yes** | **no**}**]**

Syntax Definitions

ipv6_address	Destination IPv6 address. IPv6 address of the host whose route you want to trace.
hostname	DNS name of the host whose route you want to trace.
if_name	If the target is a link-local address, the name of the interface used to reach it.
hop_count	Maximum hop count for the trace.
port_number	Specific UDP port destination. By default, the destination port is chosen by traceroute6.
probe	Number of probes to be sent to a single hop.
size	The initial size for the probe packets. During the trace the packet size will be adjusted downward as path MTU information is received. The default and maximum value is 24,000 bytes with a minimum of 1,280 bytes.
host-names {**yes** | **no**}	Specify whether each hop must be shown as an IPv6 address or the host name corresponding to the address.

Defaults

parameter	default
hop_count	32
probe	3
host-names	no

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When using this command, you must enter the name of the destination as part of the command line (either the IPv6 address or hostname).
- Use the optional **max-hop** parameter to set a maximum hop count to the destination. If the trace reaches this maximum hop count without reaching the destination, the trace stops.

Examples

```
-> traceroute6 41EA:103::65C3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ping6	Tests whether an IPv6 destination can be reached from the local switch.

MIB Objects

N/A

modify boot parameters

This command is used to configure IPv6 EMP interface.

modify boot parameters

Syntax Definitions

N/A

Defaults

By default, the EMP interface will have the following configuration.

parameter	default
baudrate	9600
parity	none
wordsize	8
stopbits	1
mode	modemControlOff

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You must be on the system console to modify the system boot parameters. Enter **modify boot parameters** command. This enters the **boot** mode. IPv6 EMP interface parameters like the unique IP address and mask, baudrate, priority, and so on can be configured after entering the boot mode.
- Only one IPv6 EMP interface is allowed per physical EMP port in the default VRF.
- It is required to configure an unique IPv6 Address that does not conflict with any other IPv6 interface configured in the system.
- It is required to reload the switch for the modified interface configuration to come into effect.

Examples

```
-> modify boot parameters
Please wait...
Type '?' for help, 'exit' to exit the boot param parser.
Boot > ?
boot empipaddr         <ip address>
boot empmasklength     <number of bits in mask>
boot serialbaudrate    <1200, 2400, 4800, 9600, 19200, 38400, 57600, 76800, 115200>
boot serialparity      <none, even, odd>
boot serialwordsize    <7, 8>
boot serialstopbits    <1, 2>
boot serialmode        <modemControlOn, modemControlOff>
boot empipv6addr       <ipv6 address>
boot empipv6masklength <number of bits in mask>
```

```
'show'           - Display the edit buffer
'commit boot'    - Commit the changes to non volatile memory for future boots
'commit system'  - Commit the changes to running system ONLY
                   Note: EMP changes will only take effect on a future boot
'exit'           - Exit (quit)
```

show command displays the existing configuration of EMP interface.

```
Boot > show
EMP IP Address            : 10.200.105.21/24
Serial (console) baud     : 9600
Serial (console) parity   : none
Serial (console) wordsize : 8
Serial (console) stopbits : 1
Serial (console) mode     : modemControlOff
EMP IPV6 Address          : /
```

To Configure IPv6 EMP interface, configure the IP address and mask:

```
Boot > boot empipv6masklength 64
Boot > show
EMP IP Address            : 10.200.105.21/24
Serial (console) baud     : 9600
Serial (console) parity   : none
Serial (console) wordsize : 8
Serial (console) stopbits : 1
Serial (console) mode     : modemControlOff
EMP IPV6 Address          : /64

Boot > boot empipv6addr  2001::205
Boot > show
EMP IP Address            : 10.200.105.21/24
Serial (console) baud     : 9600
Serial (console) parity   : none
Serial (console) wordsize : 8
Serial (console) stopbits : 1
Serial (console) mode     : modemControlOff
EMP IPV6 Address          : 2001::205/64
Boot >
```

Release History

Release 8.4.1; command introduced.

Related Commands

show ipv6 interface	Displays IPv6 interface configuration.
show ipv6 emp-interface	Displays the IPv6 EMP interface configuration.
show ipv6 emp-routes	Displays the IPv6 routes targeted to EMP port/IPv6 EMP interface configuration.

MIB Objects

N/A

show ipv6 icmp statistics

Displays IPv6 ICMP statistics.

show ipv6 icmp statistics [*if_name*]

Syntax Definitions

if_name	Display statistics only for this interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the ICMP table to monitor and troubleshoot the switch.

Examples

```
-> show ipv6 icmp statistics
Message                          Current    Previous   Change
-------------------------------+----------+----------+----------
Received Total                         857          0         857
  Errors                                 0          0           0
  Destination Unreachable                0          0           0
  Packet Too Big                         0          0           0
  Time Exceeded                          0          0           0
  Parameter Problems                     0          0           0
  Echo Requests                          0          0           0
  Echo Replies                           0          0           0
  Group Membership Queries               0          0           0
  Group Membership Responses             0          0           0
  Group Membership Reductions            0          0           0
  Router Solicitations                   9          0           9
  Router Advertisements                847          0         847
  Neighbor Solicitations                 1          0           1
  Neighbor Advertisements                0          0           0
  Redirects                              0          0           0
  Administratively Prohibited            0          0           0
Sent Total                              18          0          18
  Errors                                 0          0           0
  Destination Unreachable                0          0           0
  Packet Too Big                         0          0           0
  Time Exceeded                          0          0           0
  Parameter Problems                     0          0           0
  Echo Requests                          0          0           0
  Echo Replies                           0          0           0
  Group Membership Queries               0          0           0
  Group Membership Responses            11          0          11
  Group Membership Reductions            0          0           0
```

```
Router Solicitations                3          0          3
Router Advertisements               0          0          0
Neighbor Solicitations              4          0          4
Neighbor Advertisements             0          0          0
Redirects                           0          0          0
Administratively Prohibited         0          0          0
```

output definitions

Total	Total number of ICMPv6 messages the switch received or attempted to send.
Errors	Number of ICMPv6 messages the switch sent or received but was unable to process because of ICMPv6-specific errors (bad checksums, bad length, etc.).
Destination Unreachable	Number of Destination Unreachable messages that were sent or received by the switch.
Packet Too Big	Number of Packet Too Big messages sent or received by the switch.
Administratively Prohibited	Number of Destination Unreachable/Communication Administratively Prohibited messages sent or received by the switch.
Time Exceeded	Number of Time Exceeded messages sent or received by the switch.
Parameter Problems	Number of Parameter Problem messages sent or received by the switch.
Echo Requests	Number of Echo Request messages sent or received by the switch.
Echo Replies	Number of Echo Reply messages sent or received by the switch.
Group Membership Queries	Number of Group Membership Queries sent or received by the switch.
Group Membership Responses	Number of Group Membership Responses sent or received by the switch.
Group Membership Reductions	Number of Group Membership Reductions sent or received by the switch.
Router Solicitations	Number of Router Solicitations sent or received by the switch.
Router Advertisements	Number of Router Advertisements sent or received by the switch.
Neighbor Solicitations	Number of Neighbor Solicitations sent or received by the switch.
Neighbor Advertisements	Number of Neighbor Advertisements sent or received by the switch.
Redirects	Number of Redirect messages sent or received by the switch.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 traffic	Displays IPv6 traffic statistics.

MIB Objects

```
ipv6IfIcmpTable
   ipv6IfIcmpInMsgs
   ipv6IfIcmpInErrors
   ipv6IfIcmpInDestUnreachs
   ipv6IfIcmpInAdminProhibs
   ipv6IfIcmpInTimeExcds
   ipv6IfIcmpInParmProblems
   ipv6IfIcmpInPktTooBigs
   ipv6IfIcmpInEchos
   ipv6IfIcmpInEchoReplies
   ipv6IfIcmpInRouterSolicits
   ipv6IfIcmpInRouterAdvertisements
   ipv6IfIcmpInNeighborSolicits
   ipv6IfIcmpInNeighborAdvertisements
   ipv6IfIcmpInRedirects
   ipv6IfIcmpInGroupMembQueries
   ipv6IfIcmpInGroupMembResponses
   ipv6IfIcmpInGroupMembReductions
   ipv6IfIcmpOutMsgs
   ipv6IfIcmpOutErrors
   ipv6IfIcmpOutDestUnreachs
   ipv6IfIcmpOutAdminProhibs
   ipv6IfIcmpOutTimeExcds
   ipv6IfIcmpOutParmProblems
   ipv6IfIcmpOutPktTooBigs
   ipv6IfIcmpOutEchos
   ipv6IfIcmpOutEchoReplies
   ipv6IfIcmpOutRouterSolicits
   ipv6IfIcmpOutRouterAdvertisements
   ipv6IfIcmpOutNeighborSolicits
   ipv6IfIcmpOutNeighborAdvertisements
   ipv6IfIcmpOutRedirects
   ipv6IfIcmpOutGroupMembQueries
   ipv6IfIcmpOutGroupMembResponses
   ipv6IfIcmpOutGroupMembReductions
```

show ipv6 interface

Displays the configuration and status of IPv6 interfaces.

show ipv6 interface [*if_name* | **loopback**]

Syntax Definitions

if_name	Interface name. Limits the display to a specific interface.
loopback	Limits display to loopback interfaces.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If an interface name is not specified, all IPv6 interfaces are displayed.
- Specify an interface name (e.g., VLAN 12) to obtain a more detailed information about a specific interface.

Examples

```
-> show ipv6 interface
Name                 IPv6 Address/Prefix Length               Status    Device
-----------------+---------------------------------------+---------+-----------
smbif-5            fe80::2d0:95ff:fe12:f470/64             Active    VLAN 955
                   212:95:5::35/64
                   212:95:5::/64
if-200             fe80::eae7:32ff:fea4:6321/64            Inactive  VLAN 200
tunnel_6to4        2002:d423:2323::35/64                   Active    6to4 Tunnel
                   2002:d423:2323::/64
v6if-tunnel-137    fe80::2d0:95ff:fe12:f470/64             Disabled  Tunnel 2
                   137:35:35::35/64
                   137:35:35::/64                          Active    loopback
loopback           ::1/128                                 Active    Loopback
EMP-CMMA-CHAS1     2001::205/64                             Active   EMP
                   fe80::eae7:32ff:fea4:a1a8/64
vpn1               fe80::2b0:d0ff:fe86:880e/64             Active    Service 1
                   2001:db8:1000::2b0:d0ff:fe86:880e/64
rp-10              fe80::2b0:d0ff:fe86:880e/64             Active    VLAN 10 1/1/2
rp_11              fe80::2b0:d0ff:fe86:880e/64             Active    VLAN 11 agg 7
```

output definitions

Name	The name assigned to the IPv6 interface.
IPv6 Address/Prefix Length	IPv6 address and prefix length assigned to the interface. If an interface has more than one IPv6 address assigned to it, each address is shown on a separate line.

output definitions

Status	Interface status (Active/Inactive/Disabled).
Device	The device on which the interface is configured (for example, VLAN 955). This field will also display the port or link aggregate assignment for IPv6 routed-port interfaces (for example, “VLAN 10 1/1/2”)

```
-> show ipv6 interface if-200
if-200
  IPv6 interface index          = 200(0x000000c8)
  Administrative status         = Enabled
  Operational status            = Inactive
  Hardware address              = e8:e7:32:a4:63:21
  Device                        = VLAN 200
  Link-local address(es):
    fe80::eae7:32ff:fea4:6321/64
  Global unicast address(es):
  Anycast address(es):
  VRRP address(es):
  Joined group addresses:
    ff01::1
    ff02::1
    ff02::2
  Maximum Transfer Unit (MTU)   = 1500
  Neighbor reachable time (sec) = 346
  Base reachable time (sec)     = 360
  Retransmit timer (ms)         = 1000
  Retransmit backoff            = 1
  Retransmit max                = 3
  DAD transmits                 = 1
  Send Router Advertisements    = Yes
  Maximum RA interval (sec)     = 600
  Minimum RA interval (sec)     = 198
  RA managed config flag        = False
  RA other config flag          = False
  RA reachable time (ms)        = 0
  RA retransmit timer (ms)      = 0
  RA default lifetime (sec)     = 1800
  RA hop limit                  = 64
  RA send MTU option            = No
  RA clock skew (sec)           = 600
  RA router preference          = Medium
  RA filtering                  = Disabled
  Neighbor cache limit          = None
  Local Proxy ND                = Disabled

-> show ipv6 interface EMP-CMMA-CHAS1
EMP-CMMA-CHAS1
  IPv6 interface index          = 67108865(0x04000001)
  Administrative status         = Enabled
  Operational status            = Active
  Hardware address              = e8:e7:32:a4:a1:a8
  Device                        = EMP
  Link-local address(es):
    fe80::eae7:32ff:fea4:a1a8/64
  Global unicast address(es):
    2001::205/64
  Anycast address(es):
  VRRP address(es):
```

```
    Joined group addresses:
      ff01::1
      ff01::2
      ff02::1
      ff02::1:ff00:205
      ff02::202
      ff02::1:ffa4:a1a8
      ff02::2
      ff02::1:ff00:0
      ff05::2
    Maximum Transfer Unit (MTU)   = 1500
    Neighbor reachable time (sec) = 420
    Base reachable time (sec)     = 360
    Retransmit timer (ms)         = 1000
    Retransmit backoff            = 1
    Retransmit max                = 3
    DAD transmits                 = 1
    Send Router Advertisements    = No
    Maximum RA interval (sec)     = 600
    Minimum RA interval (sec)     = 198
    RA managed config flag        = False
    RA other config flag          = False
    RA reachable time (ms)        = 0
    RA retransmit timer (ms)      = 0
    RA default lifetime (sec)     = 1800
    RA hop limit                  = 64
    RA send MTU option            = No
    RA clock skew (sec)           = 600
    RA router preference          = Medium
    Neighbor cache limit          = None

  -> show ipv6 interface vpn1
  vpn1
    IPv6 interface index          = 100663297(0x06000001)
    Administrative status         = Enabled
    Operational status            = Inactive
    Hardware address              = e8:e7:32:1e:4c:88
    Device                        = Service 1
    Link-local address(es):
      fe80::eae7:32ff:fe1e:4c88/64
    Global unicast address(es):
      2001:db8:1000::2b0:d0ff:fe86:880e/64
    Anycast address(es):
    VRRP address(es):
    Joined group addresses:
      ff01::1
      ff02::1
      ff02::2
    Maximum Transfer Unit (MTU)   = 1500
    Neighbor reachable time (sec) = 284
    Base reachable time (sec)     = 360
    Retransmit timer (ms)         = 1000
    Retransmit backoff            = 1
    Retransmit max                = 3
    DAD transmits                 = 1
    Send Router Advertisements    = Yes
    Maximum RA interval (sec)     = 600
    Minimum RA interval (sec)     = 198
    RA managed config flag        = False
```

```
  RA other config flag          = False
  RA reachable time (ms)        = 0
  RA retransmit timer (ms)      = 0
  RA default lifetime (sec)     = 1800
  RA hop limit                  = 64
  RA send MTU option            = No
  RA clock skew (sec)           = 600
  RA router preference          = Medium
  RA filtering                  = Disabled
  Neighbor cache limit          = None
  Local Proxy ND                = Disabled

-> show ipv6 interface rp_10
rp_10
  IPv6 interface index          = 100663297(0x06000001)
  Administrative status         = Enabled
  Operational status            = Inactive
  Hardware address              = e8:e7:32:1e:4c:88
  Device                        = VLAN 10 1/1/1
  Routed Port                   = 1/1/1 tagged
  Link-local address(es):
    fe80::eae7:32ff:fe1e:4c88/64
  Global unicast address(es):
    2001:db8:1000::2b0:d0ff:fe86:880e/64
  Anycast address(es):
  VRRP address(es):
  Joined group addresses:
    ff01::1
    ff02::1
    ff02::2
  Maximum Transfer Unit (MTU)   = 1500
  Neighbor reachable time (sec) = 284
  Base reachable time (sec)     = 360
  Retransmit timer (ms)         = 1000
  Retransmit backoff            = 1
  Retransmit max                = 3
  DAD transmits                 = 1
  Send Router Advertisements    = Yes
  Maximum RA interval (sec)     = 600
  Minimum RA interval (sec)     = 198
  RA managed config flag        = False
  RA other config flag          = False
  RA reachable time (ms)        = 0
  RA retransmit timer (ms)      = 0
  RA default lifetime (sec)     = 1800
  RA hop limit                  = 64
  RA send MTU option            = No
  RA clock skew (sec)           = 600
  RA router preference          = Medium
  RA filtering                  = Disabled
  Neighbor cache limit          = None
  Local Proxy ND                = Disabled
```

output definitions

IPv6 interface index	IPv6IfIndex value that must be used in SNMP requests pertaining to this interface.
Administrative status	Administrative status of this interface (Enabled/Disabled).

output definitions (continued)

Operational status	Indicates whether the physical interface is connected to a device (Active/Inactive).
Hardware address	The hardware address.
Device	The device on which the interface is configured (for example, VLAN 955). This field will also display the port or link aggregate assignment for IPv6 routed-port interfaces (for example, "VLAN 10 1/1/2")
Routed Port	This field appears only for routed port interfaces and displays the tag status (tagged or untagged) of the port or link aggregate that is associated with the routed port interface.
Link-local address	Link-local address assigned to the interface.
Global unicast address(es)	Global unicast address(es) assigned to the interface.
Anycast address(es)	The anycast address(es) assigned to this interface.
VRRP address(es)	Addresses assigned to the interface because a VRRP virtual router is active. If (accept) is present, the switch will accept packets destined to the address. If not present, any such packets will be discarded.
Joined group address(es)	Addresses of the multicast groups that this interface has joined.
Maximum Transfer Unit	Interface MTU value.
Neighbor reachable time (sec)	The amount of time that a neighbor reached through this interface will remain in the reachable state.
Base reachable time (sec)	The base reachable time used to calculate the current neighbor reachable time.
Retransmit timer (ms)	The interval at which neighbour solicitations will be retransmitted during the neighbor discovery process.
Retransmit backoff	The NUD exponential backoff base value.
Retransmit max	The maximum number of neighbor solicitations to be sent during ND/ NUD.
DAD transmits	The number of neighbour solicitations that will be sent as part of the Duplicate Address Detection process.
Send Router Advertisements	Indicates if the router sends periodic router advertisements and responds to router solicitations on the interface.
Maximum RA interval (sec)	Maximum time between the transmission of unsolicited router advertisements over the interface.
Minimum RA interval (sec)	Minimum time between the transmission of unsolicited router advertisements over the interface (0.33 * Maximum RA Interval).
RA managed config flag	True/False value in the managed address configuration flag field in router advertisements.
RA other config flag	The True/False value in the other stateful configuration flag field in router advertisements sent over this interface.
RA reachable time (ms)	Value placed in the reachable time field in the router advertisements sent over this interface.
RA retransmit timer (ms)	Value placed in the retransmit timer field in router advertisements sent over this interface.
RA default lifetime (sec)	The value placed in the router lifetime field in the router advertisements sent over this interface.
RA hop limit	The value placed in the current hop limit field in the router advertisements sent over this interface.

output definitions (continued)

RA Send MTU option	Specifies whether the MTU option is included in the router advertisements sent over this interface.
RA clock skew (sec)	The clock skew allowed for router advertisements on this interface.
RA filtering	Specifies if RA filtering is enabled or disabled on the interface.
Neighbor cache limit	The interface's neighbor cache limit. “none” if value not set.
RA router preference	Specifies the router preference - medium, high, low.
Local Proxy ND	Specifies if Local Proxy Neighbor Discovery is enabled or disabled on the interface.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1: EMP interface information added.
Release 8.5R4; service-based interface information added.
Release 8.6R2; “Device” and “Routed Port” fields added.

Related Commands

ipv6 address	Configures an IPv6 address for an IPv6 interface.
ipv6 interface	Configures an IPv6 interface.
ipv6 interface rtr-port	Configures an IPv6 routed-port interface.
modify boot parameters	Configures the IPv6 EMP interface.

MIB Objects

```
ipv6IfTable
   ipv6IfIndex
   ipv6IfAdminStatus
   ipv6IfOperStatus
   ipv6IfPhysicalAddress
ipv6AddrTable
   ipv6AddrAddress
   ipv6AddrPfxLength
alaIPv6InterfaceAddressTable
   alaIPv6InterfaceAddress
   alaIPv6InterfaceAddressPrefixLength
   alaIPv6InterfaceAddressAnycastFlag
alaIPv6InterfaceTable
   alaIPv6InterfaceName
   alaIPv6InterfaceDescription
   alaIPv6InterfaceAddressVRRPFlag
   alaIPv6MulticastGroupAddress
   alaIPv6InterfaceMtu
   alaIPv6InterfaceReachableTime
   alaIPv6InterfaceBaseReachableTime
   alaIPv6InterfaceRetransTimer
   alaIPv6InterfaceRetransBackoff
   alaIPv6InterfaceRetransMax
   alaIPv6InterfaceDADTransmits
   alaIPv6InterfaceSendRouterAdvertisements
   alaIPv6InterfaceMaxRtrAdvInterval
   alaIPv6InterfaceMinRtrAdvInterval
   alaIPv6InterfaceAdvManagedFlag
   alaIPv6InterfaceAdvOtherConfigFlag
   alaIPv6InterfaceAdvReachableTime
   alaIPv6InterfaceAdvRetransTimer
   alaIPv6InterfaceAdvDefaultLifetime
   alaIPv6InterfaceAdvHopLimit
   alaIPv6InterfaceAdvSendMtu
   alaIPv6InterfaceClockSkew
   alaIPv6InterfaceRAFilter
   alaIPv6InterfaceNeighborLimit
   alaIPv6InterfaceLPND
```

show ipv6 emp-interface

Displays the IPv6 EMP interface configuration.

show ipv6 emp-interface

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 emp-interface
Name                IPv6 Address/Prefix Length               Status    Device
--------------------+----------------------------------------+---------+--------
EMP-CMMA-CHAS1      2001::205/64                              Active    EMP
                    fe80::eae7:32ff:fea4:a1a8/64
```

output definitions

Name	Interface name.
IPv6 Address/Prefix Length	IPv6 address and prefix length assigned to the interface. If an interface has more than one IPv6 address assigned to it, each address is shown on a separate line.
Status	Interface status (Active/Inactive/Disabled).
Device	The device on which the interface is configured.

Release History

Release 8.4.1; command introduced.

Related Commands

modify boot parameters	This command is used to configure IPv6 EMP interface.

MIB Objects

N/A

show ipv6 emp-routes

Displays the IPv6 routes targeted to EMP port/IPv6 EMP interface configuration.

show ipv6 emp-routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 emp-routes
Legend: Flags: U=Up, G=Gateway, H=Host, S=Static, C=Cloneable, B=Discard, E=ECMP

Total 2 routes

Destination/Prefix  Gateway Address    Interface      Age    Protocol   Flags
------------------+---------------+--------------+-------+----------+------
2001::/64             ::            EMP-CMMA-CHAS1  1d 1h    LOCAL      UC
4001::/64             2001::9       EMP-CMMA-CHAS1  1d 1h    STATIC     UGS
```

output definitions

Destination/Prefix	The destination IPv6 address of the IPv6 EMP route.
Gateway Address	The next hop IPv6 address to reach the destination.
Interface	The interface through which the destination IPv6 address is reachable.
Age	Time since this route was last updated or otherwise determined to be correct.
Protocol	The routing mechanism through which this route was learned. For EMP routes, this can be only local or static. Routing protocol are not supported on EMP interface.
Flags	Route flags that describes the route details.

Release History

Release 8.4.1; command introduced.

Related Commands

ipv6 static-route	Configures an IPv6 static route.

MIB Objects

```
ipv6RouteDestipv6RoutePfxLength
ipv6RouteNextHop
alaIPv6InterfaceName
ipv6RouteAge
ipv6RouteProtocol
```

show ipv6 pmtu table

Displays the IPv6 Path MTU Table.

show ipv6 pmtu table

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pmtu table

1-PMTU Entry
PMTU entry minimum lifetime = 10m
Destination Address                                      MTU      Expires
---------------------------------------------------------+--------+-------
fe80::02d0:c0ff:fe86:1207                                1280     1h 0m
```

output definitions

Destination Address	IPv6 address of the path's destination.
MTU	Path’s MTU.
Expires	Minimum remaining lifetime for the entry.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pmtu-lifetime	Configures the minimum lifetime for entries in the path MTU Table.

MIB Objects

```
alaIPv6ConfigTable
   alaIPv6PMTUDest
   alaIPv6PMTUexpire
```

show ipv6 ra-filter

Displays the RA filter configuration for an IPv6 interface.

show ipv6 ra-filter [*if-name***]**

Syntax Definitions

if_name	IPV6 interface name.

Defaults

By default, the RA filter configuration is displayed for all IPv6 VLAN interfaces.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900

Usage Guidelines

Use the *if-name* parameter to display information for a specific IPv6 interface.

Examples

```
-> show ipv6 ra-filter
Interface                       Status   Trusted Ports
--------------------------------+--------+--------------------------------------
vlan-23                         Enabled  1/1/22, agg 7
vlan-24                         Enabled  none
```

output definitions

Interface	Displays the IPv6 VLAN interface on which RA filtering is configured.
Status	Displays the status of RA filtering on the interface. The interfaces on which the RA filtering is disabled are displayed only if one or more trusted ports are configured for the interface.
Trusted Ports	Displays the RA filtering trusted sources for the interface. A '+' will appear at the end of the list to indicate that there are more trusted sources configured which cannot be displayed in a single line. To view the full list of configured trusted sources, specify the interface name in the **show** command as recommended.

```
-> show ipv6 ra-filter vlan-23
RA Filtering: Enabled
Trusted ports:
  1/1/22
  linkagg 7
```

output definitions

RA Filtering	Indicates if RA filtering is enabled or disabled on the IPv6 VLAN interface.
Trusted ports	Shows the RA filtering trusted ports (chassis/slot/port) or link aggregates (linkagg ID) for the interface. Displays **none** if there are no trusted ports.

Release History

Release 8.1.1; command introduced.
Release 8.5R2; OmniSwitch 6560 support for IPv6 RA Filtering added.

Related Commands

ipv6 ra-filter	Enables or disables the status of RA filtering on IPv6 VLAN interfaces. When enabled, any RAs received on associated ports and link aggregates are discarded.
ipv6 ra-filter trusted	Configures the RA filtering trust status for ports and link aggregates associated with the IPv6 VLAN interface. When a port or link aggregate is trusted, it can accept RAs received when the RA filtering status is enabled.

MIB Objects

```
IPv6IfIndex
   alaIPv6RAFilterTrustedChassis
   alaIPv6RAFilterTrustedSlot
   alaIPv6RAFilterTrustedPort
```

show ipv6 neighbors

Displays IPv6 Neighbor Table.

show ipv6 neighbors [*ipv6_prefix/prefix_length* | *if_name* | **hw** *hardware_address* | **static]**

Syntax Definitions

ipv6_prefix/prefix_length	IPv6 prefix. Restricts the display to those neighbors starting with the specified prefix.
if_name	Interface name. Restricts the display to those neighbors reached through the specified interface.
hardware_address	MAC address. Restricts the display to the specified MAC address.
static	Restricts display to statically configured neighbors.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If you do not specify an option (e.g., if_name), all IPv6 neighbors are displayed.

Examples

```
-> show ipv6 neighbors

Total 4 neighbors

IPv6 Address            Hardware Address  Reachability Lifetime Port           Interface
------------------------+-----------------+------------+--------+--------------+---------
2001:db8:9::88          00:d0:95:01:0a:ec Confirmed       5m 5s 1/3/7          vlan_7
fe80::2d0:95ff:fe01:aec 00:d0:95:01:0a:ec Confirmed       5m 6s 1/3/7          vlan_7
2001:db8:1000::100      00:d0:95:a8:08:11 Confirmed      2m 20s sap:1/3/9:1000 vpn1
2001:db8:1000::101      00:d0:95:c3:19:aa Confirmed      1m 23s sdp:32768:1000 vpn1
```

output definitions

IPv6 Address	The neighbor's IPv6 address.
Hardware Address	The MAC address corresponding to the IPv6 address.
Reachability	The neighbor's reachability: • Incomplete • Confirmed • Unconfirmed
Lifetime	The time the entry will remain in its current state.
Port	The port used to reach the neighbor.
Interface	The neighbor's interface name (e.g., vlan_1).

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; neighbor information for service-based interfaces added.

Related Commands

ipv6 neighbor	Configures a static entry in the IPv6 Neighbor Table.

MIB Objects

```
ipv6IfIndex
alaIPv6NeighborTable
   alaIPv6NeighborNetAddress
   alaIPv6NeighborPhysAddress
   alaIPv6NeighborReachability
   alaIPv6NeighborLifetime
   alaIPv6NeighborType
   alaIPv6NeighborPortIfIndex
   alaIPv6NeighborPortType
   alaIPv6NeighborPortSubId
```

clear ipv6 neighbors

Removes all entries, except static entries, from IPv6 Neighbor Table.

clear ipv6 neighbors

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command only clears dynamic entries. If static entries have been added to the table, they must be removed using the **no** form of the **ipv6 neighbor** command.

Examples

```
-> clear ipv6 neighbors
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 neighbor	Configures a static entry in IPv6 Neighbor Table.
show ipv6 neighbors	Displays IPv6 Neighbor Table.

MIB Objects

```
alaIPv6NeighborTable
   alaIPv6ClearNeighbors
```

show ipv6 prefixes

Displays IPv6 prefixes used in router advertisements.

show ipv6 prefixes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 prefixes

Legend: Flags: A = Autonomous Address Configuration, L = OnLink

                                          Valid     Preferred
Name           IPv6 Address/Prefix Length   Lifetime   Lifetime   Flags   Source
---------------+----------------------------+----------+----------+-------+---------
vlan 955       212:95:5::/64                 2592000    604800     LA     dynamic
vlan 1002      195:35::/64                   2592000    604800     LA     dynamic
6to4tunnel     2002:d423:2323::/64           2592000    604800     LA     dynamic
tunnel 2       137:35:35::/64                2592000    604800     LA     dynamic
```

output definitions

Name	The interface name. This is usually the VLAN on which the interface is configured.
IPv6 Address/Prefix Length	The IPv6 prefix and prefix length for a Router Advertisement Prefix Option.
Valid Lifetime	Length of time, in seconds, that this prefix will remain valid (i.e., time until deprecation). A value of 4,294,967,295 represents infinity.
Preferred Lifetime	Length of time, in seconds, that this prefix will remain preferred (i.e. time until deprecation). A value of 4,294,967,295 represents infinity.
Flags	**L** - Prefix can be used for onlink determination. **A** - Prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
Source	**config** - Prefix has been configured by management. **dynamic** - Router Advertisements are using interface prefixes.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 prefix	Configures an IPv6 prefix on an interface. Used for configuring prefixes for router advertisements.

MIB Objects

```
IPv6AddrPrefixTable
   IPv6AddressPrefixEntry
   IPv6AddressPrefixLength
   IPv6AddressPrefixLinkFlag
   IPv6AddressPrefixAdvvalidLifetime
   IPv6AddressPrefixAdvPreferredLifetime
alaIPv6InterfacePrefixTable
   alaIPv6InterfacePrefix
   alaIPv6InterfacePrefixLength
   alaIPv6InterfacePrefixValidLifetime
   alaIPv6InterfacePrefixPreferredLifetime
   alaIPv6InterfacePrefixOnLinkFlag
   alaIPv6InterfacePrefixsource
```

show ipv6 routes

Displays IPv6 Forwarding Table.

show ipv6 routes [*ipv6_prefix/prefix_length* **| summary | protocol [bgp| import | isis | local | ospf | rip static]]**

Syntax Definitions

ipv6_prefix/prefix_length	IPv6 prefix. Restricts the display to those routes starting with the specified prefix.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

show ipv6 routes does not include the EMP interface included in the total routes count.

Examples

```
-> show ipv6 routes
Legend: Flags: U=Up, G=Gateway, H=Host, S=Static, C=Cloneable, B=Discard, E=ECMP

Total 5 routes

Destination Prefix  Gateway Address           Interface         Age          Protocol  Flags
--------------------+---------------+--------+-----------------+------------+---------+-----
::/0                2002:d468:8a89::137       v6if-6to4-137     18h 47m 26s  Static    UGS
137:35:35::/64      fe80::2d0:95ff:fe12:f470  v6if-tunnel-137   18h 51m 55s  Local     UC
195:35::/64         fe80::2d0:95ff:fe12:f470  v6if-to-eagle     18h 51m 55s  Local     UC
212:95:5::/64       fe80::2d0:95ff:fe12:f470  smbif-5           18h 51m 55s  Local     UC
55::/64             ::                        loopback          00:00:13     STATIC    UBS
```

output definitions

Destination Prefix	IPv6 destination address and prefix.
Gateway Address	IPv6 address of the gateway used to reach the destination network. Gateway address '::' indicates an IPv6 blackhole route.
Interface	The device the interface is using (e.g., VLAN 6to4tunnel); or loopback.
Age	Age of the entry. Entries less than 1 day old are displayed in hh:mm:ss format. Entries more than 1 day old are displayed in dd:hh format.
Protocol	Protocol by which the route was learned.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 static-route	Configures a static entry in the IPv6 route.

MIB Objects

```
IPv6RouteTable
   IPv6Routes
   IPv6RoutesPrefix
   IPV6RoutesStatic
alaIPv6StaticRouteTable
   alaIPv6StaticRouteEntry
```

show ipv6 route-pref

Displays the IPv6 routing preference of the router.

show ipv6 route-pref

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The IPv6 version of BGP is not supported on the OmniSwitch 6560 or OmniSwitch 6465.

Examples

```
-> show ipv6 route-pref
  Protocol    Route Preference Value
------------+-----------------------
  Local                   1
  Static                  2
  OSPF                  110
  ISISL1                115
  ISISL2                118
  RIP                   120
  EBGP                  190
  IBGP                  200
  Import                210
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 route-pref	Configures the IPv6 route preference of a router.

MIB Objects

N/A

show ipv6 router database

Displays a list of all routes (static and dynamic) that exist in the IPv6 router database. This database serves as a central repository where routes are first processed for redistribution and where duplicate routes are compared to determine the best route to use. If a route does not appear in the IPv6 router database list, then the switch does not know about it. In the case of dynamically learned routes, this could indicate that the route was never received by the switch.

show ipv6 router database [protocol *type* | **gateway** *ipv6_address* | **dest** *ipv6_prefix/prefix_length***]**

Syntax Definitions

type	Routing protocol type (local, static, OSPF, RIP, BGP, IS-IS, or IMPORT).
ipv6_address	IPv6 address of the next hop used to reach the destination IPv6 address.
ipv6_prefix	IPv6 network that is the destination of this static route.
/prefix_length	The number of bits that are significant in the iPv6 address (mask). (0...128).

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The IPv6 forwarding table is derived from IPv6 router database processing performed by the switch and contains only unique routes that the switch currently uses. Use the **show ipv6 routes** command to view the forwarding table.
- If an expected route does not appear in the IPv6 forwarding table, use the **show ipv6 router database** command to see if the switch knows about the route and/or if a duplicate route with a higher precedence was selected instead.
- The switch compares the protocol of duplicate routes to determine which one to use. Regardless of whether or not a route has a higher priority metric value, protocol determines precedence. Local routes are given the highest level of precedence followed by static, OSFP, RIP, then BGP routes. As a result, a route that is known to the switch may not appear in the IP forwarding table if a duplicate route with a higher protocol precedence exists.
- A list of inactive static routes is also included in the **show ipv6 router database** output display. A route becomes inactive if the interface for its gateway goes down. Inactive routes are unable to get to their destination and further investigation is warranted to determine why their gateway is unavailable.
- Routes that appear as inactive are not included in the main IP router database listing. If an inactive route becomes active, however, it is removed from the inactive list and added to the active route list.

Examples

```
-> show ipv6 router database
Legend: + indicates routes in use
        b indicates BFD-enabled static route

Total IPRM IPv6 routes: 4

Destination/Prefix    Gateway Address             Interface   Protocol    Metric    Tag
------------------+--------------------------+-----------+-----------+---------+--------
+  2001::/64          fe80::2efa:a2ff:fe23:24ca   VL-2059      OSPF         1        0
+  2001::/64          fe80::de08:56ff:fe10:b41    VL-2060      OSPF         1        0
+  2001:0:1::/64      fe80::2efa:a2ff:fe23:24ca   VL-2059      OSPF         2        0
+  55::/6             ::                          loopback     STATIC       10       0

Inactive Static Routes:
Vlan  Destination/Prefix       Gateway Address               Metric       Tag
-----+---------------------+----------------------------+------------+--------
1510  212:95:5::/64            fe80::2d0:95ff:fe6a:f458        1           0
```

output definitions

Destination/Prefix	IPv6 destination address and prefix.
Gateway Address	IPv6 address of the gateway used to reach the destination network. Gateway address '::' indicates an IPv6 blackhole route.
Interface	The device the interface is using (e.g., VLAN 6to4tunnel); or loopback.
Protocol	Protocol by which this IPv6 address was learned: LOCAL, STATIC, OSPF, RIP, BGP).
Metric	RIP metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.
VLAN	The VLAN on which the route was *learned*, not forwarded. Note that **N/A** appears in this field for static routes as they are not learned on a VLAN.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 routes	Displays the IPv6 Forwarding Table.

MIB Objects

N/A

show ipv6 tcp connections

Displays the TCP connections over the IPV6 table.

show ipv6 tcp connections

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 tcp connections

Local Address               Port  Remote Address               Port   State
----------------------------+-----+----------------------------+-----+------
2001:0000:0200::23            23  2001:0000:0400::143          1867   established
2001:0000:0200::23          8734  2001:0000:0200::19           8735   timeWait
```

output definitions

Local Address	The local IPV6 address for the TCP connection .
Port	The local port number of the TCP connection.
Remote Address	The remote IPV6 address for the TCP connection.
Port	The remote port number of the TCP connection.
State	The state of the TCP connection.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 tcp listeners	Displays the TCP connections over the IPV6 listeners (endpoints awaiting a connection request).

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceStatus
   alaRipngRouteTag
   alaRipngInvalidTimer
   alaRipngGarbageTimer
   alaRipngHolddownTimer
   alaRipngJitter
   alaRipngTriggeredSends
```

show ipv6 tcp listeners

Displays the TCP connections over the IPV6 listeners (endpoints awaiting a connection request).

show ipv6 tcp listeners

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 tcp listeners

Local Address                                Port
---------------------------------------------+-----
::0                                            21
::0                                            23
::0                                            80
```

output definitions

Local Address	The local IPV6 address for this TCP listener. A value of ::0 indicates that the listener will accept a connection request sent to any of the switch's addresses.
Port	The local port number on which the listener is awaiting connection requests.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 tcp connections	Displays the TCP connections over the IPV6 table.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceStatus
   alaRipngRouteTag
   laRipngInvalidTimer
   alaRipngGarbageTimer
   alaRipngHolddownTimer
   alaRipngJitter
   alaRipngTriggeredSends
```

show ipv6 traffic

Displays IPv6 traffic statistics.

show ipv6 traffic [*if_name*]

Syntax Definitions

if_name	Interface name. Restricts the display to the specified interface instead of global statistics.

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The statistics show the cumulative totals since the last time the switch was powered on, the last reset of the switch was executed or the traffic statistics were cleared using the command.

Examples

```
-> show ipv6 traffic
Message                   Current    Previous   Change
------------------------+----------+----------+----------
Packets received
  Total                     66193          0      66193
  Header errors                 0          0          0
  Too big                       0          0          0
  No route                      0          0          0
  Address errors                0          0          0
  Unknown protocol              0          0          0
  Truncated packets             0          0          0
  Local discards                0          0          0
  Delivered to users          969          0        969
  Reassembly needed             0          0          0
  Reassembly failed             0          0          0
  Multicast packets         66191          0      66191
Packets sent
  Forwarded                     0          0          0
  Generated                    23          0         23
  Local discards                5          0          5
  Fragmented                    0          0          0
  Fragmentation failed          0          0          0
  Fragments generated           0          0          0
  Multicast packets            34          0         34
```

output definitions

Total	Total number of input packets received, including those received in error.
Header errors	Number of input packets discarded due to errors in their IPv6 headers (e.g., version number mismatch, other format errors, hop count exceeded, and errors discovered in processing their IPv6 options).
Too big	Number of input packets that could not be forwarded because their size exceeded the link MTU of the outgoing interface.
No route	Number of input packets discarded because no route could be found to transmit them to their destination.
Address errors	Number of input packets discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes).
Unknown protocol	Number of locally-addressed packets received successfully but discarded because of an unknown or unsupported protocol.
Truncated packets	Number of input packets discarded because the packet frame did not carry enough data.
Local discards	Number of input IPv6 packets for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any packets discarded while awaiting re-assembly.
Delivered to users	Total number of packets successfully delivered to IPv6 user protocols (including ICMP).
Reassembly needed	Number of IPv6 fragments received that needed to be reassembled.
Reassembly failed	Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.).
Multicast packets	Number of multicast packets received.
Forwarded	Number of output packets that this entity received and forwarded to their final destinations.
Generated	Total number of IPv6 packets that local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any packets counted by the Forwarded statistic.
Local discards	Number of output IPv6 packets for which no problem was encountered to prevent their transmission to their destination, but were discarded (e.g., for lack of buffer space). Note that this counter would include packets counted by the Forwarded statistic if any such packets met this (discretionary) discard criterion.
Fragmented	Number of IPv6 packets successfully fragmented.
Fragmentation failed	Number of IPv6 packets discarded because they needed to be fragmented but could not be.
Fragments generated	Number of output packet fragments generated as a result of fragmentation.
Multicast packets	Number of multicast packets transmitted.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 icmp statistics	Displays IPv6 ICMP statistics.

MIB Objects

```
ipv6IfStatsTable
   ipv6IfStatsInReceives
   ipv6IfStatsInHdrErrors
   ipv6IfStatsInTooBigErrors
   ipv6IfStatsInNoRoutes
   ipv6IfStatsInAddrErrors
   ipv6IfStatsInUnknownProtos
   ipv6IfStatsInTruncatedPkts
   ipv6IfStatsInDiscards
   ipv6IfStatsInDelivers
   ipv6IfStatsOutForwDatagrams
   ipv6IfStatsOutRequests
   ipv6IfStatsOutDiscards
   ipv6IfStatsOutFragOKs
   ipv6IfStatsOutFragFails
   ipv6IfStatsOutFragCreates
   ipv6IfStatsReasmReqds
   ipv6IfStatsReasmOKs
   ipv6IfStatsReasmFails
   ipv6IfStatsInMcastPkts
   ipv6IfStatsOutMcastPkts
```

show ipv6 tunnel configured

Displays IPv6 tunnel information and whether the 6to4 tunnel is enabled.

show ipv6 tunnel configured

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 tunnel configured

IPv6 6to4 tunnel: Enabled
Configured Tunnels:
Tunnel              IPv6 Address/Prefix Length    Source IPv4     Destination IPv4
--------------------+-----------------------------+---------------+-----------------
1                   2001:0000:0200::101/48        192.16.10.101   192.28.5.254
23                  2001:0000:0200::102/48        192.15.10.102   10.27.105.25
v6if-tunnel-137     fe80::2d0:95ff:fe12:f470/64   212.35.35.35    212.104.138.137
```

output definitions

IPv6 6to4 tunnel	Indicates whether 6to4 tunneling is enabled or disabled on the switch.
Tunnel	Tunnel ID.
IPv6 Address/Prefix Length	IPv6 address associated with the tunnel.
Source IPv4	Source IPv4 address for the tunnel.
Destination IPv4	Destination IPv4 address for the tunnel.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 interface	Configures an IPv6 interface on a VLAN or IPv6 tunnel.

MIB Objects

```
alaIPv6ConfigTunnelTable
   alaIPv6Tunnel6to4
   alaIPv6ConfigTunnelv4Source
   alaIPv6ConfigTunnelv4Dest
```

show ipv6 tunnel 6to4

Displays IPv6 tunnel information and whether the 6to4 tunnel is enabled.

show ipv6 tunnel 6to4

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 tunnel 6to4
tunnel_6to4
  Status = Disabled
  IPv6 Address(es):
  Local IPv4 Address(es):
```

output definitions

Name	Indicates whether 6to4 tunneling is enabled or disabled on the switch.
Status	Tunnel ID.
IPv6 Address(es)	IPv6 address associated with the tunnel.
Local IPv4 Addresses(es)	Source IPv4 address for the tunnel.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 interface	Configures an IPv6 interface on a VLAN or IPv6 tunnel.

MIB Objects

```
alaIPv6ConfigTunnelTable
   alaIPv6Tunnel6to4
   alaIPv6ConfigTunnelv4Source
   alaIPv6ConfigTunnelv4Dest
```

show ipv6 udp ports

Displays UDP Over IPv6 Listener Table. This table contains information about UDP/IPv6 endpoints.

show ipv6 udp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Only endpoints utilizing IPv6 addresses are displayed in this table.

Examples

```
-> show ipv6 udp ports

Local Address                                Port  Interface
---------------------------------------------+-----+-------------------
::                                            521
```

output definitions

Local Address	Local IPv6 address for this UDP listener. If a UDP listener accepts packets for any IPv6 address associated with the switch, the value is ::0.
Port	Local Port number for the UDP connection.
Interface	Name of the interface the listener is using or “unknown.”

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 routes	Displays TCP Over IPv6 Connection Table.

MIB Objects

```
IPv6UdpTable
   IPv6UdpEntry
   IPv6UdpLocalAddress
   IPv6UdpLocalPort
   IPv6UdpIfIndex
```

show ipv6 information

Displays IPv6 information.

show ipv6 information

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 information
Default hop limit                     = 64
Path MTU entry minimum lifetime (min) = 10
Neighbor stale lifetime (min)         = 10
Local Unicast Global ID               = none
Use VRRP virtual source MAC           = Off
Neighbor cache limit                  = None
VRF neighbor cache limit              = None
Ignore anycast echo requests          = No
Ignore multicast echo requests        = No
ICMPv6 error rate limit interval (ms) = 10
ICMPv6 error rate limit burst         = 10
```

output definitions

Default hop limit	The value placed in the hop limit field in router advertisements
Path MTU entry minimum lifetime	Minimum lifetime for entries in the path MTU.
Neighbor stale lifetime	Minimum lifetime for neighbor entries in the stale state.
Local Unicast Global ID	The default global ID value used in unique local unicast addresses. "none" if a global ID has not been configured.
Use VRRP virtual source MAC	If On, when a packet's source address is a VRRP virtual IPv6 address, the corresponding VRRP virtual MAC will be used as the source MAC address. If Off, the interface's real MAC will be used as the source MAC address.
Neighbor cache limit	The system-wide neighbor cache limit. If this value is not set: • “64” is displayed on the OmniSwitch 6465. • “128” is displayed on the OmniSwitch 6560. • “none” is displayed on all other supported OmniSwitch platforms.

output definitions

VRF neighbor cache limit	The neighbor cache limit in use for the VRF in which the command was executed. If this value is not set: • "64" is displayed on the OmniSwitch 6465. • "128" is displayed on the OmniSwitch 6560. • "none" is displayed on all other supported OmniSwitch platforms.
Ignore anycast echo requests	States whether the echo reply to anycast echo request is set to Yes or No. If set to Yes, echo replies will not be sent in response to an echo request sent to an anycast address. If set to No, the switch will reply to all anycast echo requests.
Ignore multicast echo requests	States whether the echo reply to multicast echo request is set to Yes or No. If set to Yes, echo replies will not be sent in response to an echo request sent to an multicast address. If set to No, the switch will reply to multicast echo requests.
ICMPv6 error rate limit interval	The rate limit interval in milliseconds.
ICMPv6 error rate limit burst	The maximum ICMPv6 error message burst size.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **ignore anycast echo requests**, **ignore multicast echo requests**, **ICMPv6 error rate limit interval**, **ICMPv6 error rate limit burst** fields added.

Related Commands

ipv6 neighbor	Configures a static entry in the IPv6 Neighbor Table.
ipv6 pmtu-lifetime	Configures the minimum lifetime for entries in the path MTU Table.
ipv6 hop-limit	Configures the value placed in the hop limit field in the header of all IPv6 packet.
ipv6 address global-id	Configures the default global ID for unique local unicast addresses
ipv6 echo	Configures the switch to reply or ignore echo requests in response to an echo request sent to a multicast or anycast IPv6 address.

MIB Objects

```
ipv6MibObjects
   Ipv6DefaultHopLimit
alaIPv6ConfigTable
   alaIPv6PMTUMinLifetime
alaIPv6NeighborTable
   alaIPv6NeighborStaleLifetime
```

ipv6 redist

Controls the conditions for redistributing IPv6 routes between different protocols.

ipv6 redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} {all-routes | route-map *route_map_name***} [admin-state {enable | disable}]**

no ipv6 redist {local | static | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} [all-routes | route-map *route_map_name***]**

Syntax Definitions

local	Redistributes local IPv6 routes.
static	Redistributes static IPv6 routes.
rip	Specifies RIP as the source or destination (into) protocol.
ospf	Specifies OSPF as the source or destination (into) protocol (*OSPF* is *not supported on the OmniSwitch 6465 or OmniSwitch 6560*).
isis	Specifies IS-IS as the source or destination (into) protocol (*IS-IS* is *not supported on the OmniSwitch 6465, OmniSwitch 6560, or* OmniSwitch 9900).
bgp	Specifies BGP as the source or destination (into) protocol (*BGP* is *not supported on the OmniSwitch 6465 or OmniSwitch 6560*).
import	Redistributes imported routes to other routing protocols.
all-routes	Redistributes all routes. This option does not allocate route-map resources.
route_map_name	Name of an existing route map that will control the redistribution of routes between the source and destination protocol.
enable	Enables the administrative status of the redistribution configuration.
disable	Disables the administrative status of the redistribution configuration.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a route map redistribution configuration. Note that if a route map name is not specified, all route maps associated with the redistribution configuration are removed.
- The source and destination protocols must be loaded and enabled before redistribution occurs.
- The IPv6 version of BGP is not supported in the current release.

- Use the **ip route-map** commands described in the “IP Commands” chapter of this guide to create a route map. Refer to the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.

Examples

```
-> ipv6 redist rip into ospf route-map rip-to-ospf1
-> ipv6 redist rip into ospf route-map rip-to-ospf2
-> no ipv6 redist rip into ospf route-map rip-to-ospf2
-> ipv6 redist local into rip route-map local-to-rip
-> ipv6 redist local into rip route-map local-to-rip disable
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; **all-routes** parameter added.
Release 8.5R1; **import** parameter added.

Related Commands

show ipv6 redist	Displays the route map redistribution configuration.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistSrcProtoId
   alaRouteMapRedistDestProtoId
   alaRouteMapRedistRouteMapIndex
   alaRouteMapRedistStatus
   alaRouteMapRedistAddressType
   alaRouteMapRedistRowStatus
```

ipv6 access-list

Creates an IPv6 access list that is used to specify multiple IPv6 addresses for a route map configuration.

ipv6 access-list *access_list_name*

no ipv6 access-list *access_list_name*

Syntax Definitions

access_list_name	Name of the IPv6 access list (up to 20 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to delete the access list.

Examples

```
-> ipv6 access-list access1
-> no ipv6 access-list access1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 access-list address	Adds IPv6 addresses to an existing IPv6 access list.
show ipv6 access-list	Displays the contents of an IPv6 access list.

MIB Objects

```
alaRouteMapAccessListNameTable
   alaRouteMapAccessListName
   alaRouteMapAccessListNameIndex
   alaRouteMapAccessListNameAddressType
   alaRouteMapAccessListNameRowStatus
```

ipv6 access-list address

Adds IPv6 addresses to the specified IPv6 access list.

ipv6 access-list *access_list_name* **address** *address/prefixLen* **[action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]**

no ipv6 access-list *access_list_name* **address** *address/prefixLen*

Syntax Definitions

access_list_name	Name of the IPv6 access list (up to 20 characters).
address/prefixLen	IPv6 address along with the prefix length to be added to the access list.
permit	Permits the IPv6 address for redistribution.
deny	Denies the IPv6 address for redistribution.
all-subnets	Redistributes or denies all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Redistributes or denies only those routes that exactly match the IP address and the mask length.
aggregate	Redistributes an aggregate route if there are one or more routes that match or are subnets of this address.

Defaults

parameter	default
permit | deny	**permit**
all-subnets | no-subnets | aggregate	**all-subnets**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the address from the access list.
- The *access_list_name* should exist before you add multiple IPv6 addresses to the IPv6 access list.
- The **action** parameters (**permit** and **deny**) determine if a route that matches the **redist-control** configuration for the IP address is allowed or denied redistribution.
- The **redist-control** parameters (**all-subnets, no-subnets**, and **aggregate**) defines the criteria used to determine if a route matches an address in the access list.
- Note that configuring the combination of **redist-control aggregate** with **action deny** is not allowed.
- Use this command multiple times with the same access list name to add multiple addresses to the existing IPv6 access list.

Examples

```
-> ipv6 access-list access1 address 2001::1/64 action permit
-> ipv6 access-list access1 address 2001::1/64 redist-control aggregate
-> no ipv6 access-list access1 address 2001::1/64
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 access-list	Creates an IPv6 access list that is used to specify multiple IPv6 addresses for a route map configuration.
show ipv6 access-list	Displays the contents of an IPv6 access list.

MIB Objects

```
alaRouteMapAccessListTable
   alaRouteMapAccessListIndex
   alaRouteMapAccessListAddress
   alaRouteMapAccessListAddressType
   alaRouteMapAccessListPrefixLength
   alaRouteMapAccessListAction
   alaRouteMapAccessListRedistControl
   alaRouteMapAccessListRowStatus
```

show ipv6 redist

Displays the IPv6 route map redistribution configuration.

show ipv6 redist [rip | ospf | bgp]

Syntax Definitions

rip	Displays the route map redistribution configurations that specify RIP as the destination (into) protocol.
ospf	Displays the route map redistribution configurations that specify OSPF as the destination (into) protocol.
bgp	This parameter is not supported.

Defaults

By default all route map redistribution configurations are shown.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Specify a destination protocol with this command to display only those configurations that redistribute routes into the specified protocol.
- The IPv6 version of BGP is not supported in the current release.

Release History

Release 7.1.1; command was introduced.

Examples

```
-> show ipv6 redist

Source       Destination
Protocol     Protocol     Status    Route Map
------------+------------+---------+--------------------
localIPv6    RIPng        Enabled   ipv6rm
RIPng        OSPFv3       Enabled   ipv6rm

-> show ipv6 redist ospf

Source       Destination
Protocol     Protocol     Status    Route Map
------------+------------+---------+--------------------
RIPng        OSPFv3       Enabled   ipv6rm
```

output definitions

Source Protocol	The protocol from which the routes are learned.
Destination Protocol	The protocol into which the source protocol routes are redistributed.
Status	The administrative status (**Enabled** or **Disabled**) of the route map redistribution configuration.
Route Map	The name of the route map that is applied with this redistribution configuration.

Related Commands

ipv6 redist	Controls the conditions for redistributing IPv6 routes between different protocols.

MIB Objects

```
alaRouteMapRedistProtoTable
   alaRouteMapRedistSrcProtoId
   alaRouteMapRedistDestProtoId
   alaRouteMapRedistRouteMapIndex
   alaRouteMapRedistStatus
   alaRouteMapRedistAddressType
   alaRouteMapRedistRowStatus
```

show ipv6 access-list

Displays the contents of the specified IPv6 access list.

show ipv6 access-list [*access_list_name***]**

Syntax Definitions

access_list_name	Name of the IPv6 access list.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the *access_list_name* is not specified in this command, all the access lists will be displayed.

Examples

```
-> show ipv6 access-list
                    Address /                   Redistribution
Name                Prefix Length      Effect   Control
--------------------+------------------+-------+-------------
al_3                128::/64           permit   all-subnets
al_4                124::/64           permit   no-subnets

-> show ipv6 access-list 4

                    Address /                   Redistribution
Name                Prefix Length      Effect   Control
--------------------+------------------+-------+-------------
al_4                124::/64           permit   no-subnets
```

output definitions

Name	Name of the IPv6 access list.
Address/Prefix Length	IPv6 address that belongs to the access list.
Effect	Indicates whether the IPv6 address is permitted or denied for redistribution.
Redistribution Control	Indicates the conditions specified for redistributing the matched routes.

Release History

Release 7.1.1; command was introduced

Related Commands

ipv6 access-list	Creates an IPv6 access list for adding multiple IPv6 addresses to route maps.
ipv6 access-list address	Adds multiple IPv6 addresses to the IPv6 access list.

MIB objects

```
alaRouteMapAccessListIndex
   alaRouteMapAccessListAddressType
   alaRouteMapAccessListAddress
   alaRouteMapAccessListPrefixLength
   alaRouteMapAccessListAction
   alaRouteMapAccessListRedistControl
```

ipv6 export

Exports IPv6 routes from the source VRF to the Global Routing Table (GRT) or to all VRF instances. All routes are exported or a route map can be specified to filter exported routes

[vrf *vrf_name***] ipv6 export {all-routes | route-map** *route_map_name* | **to-all-vrfs {all-routes | route-map** *route_map_name***}}**

[vrf *vrf_name***] no ipv6 export**

Syntax Definitions

vrf_name	The name of an existing VRF instance. Routes are exported from this source VRF to the GRT.
all-routes	Exports all routes from the source VRF to the GRT. This option does not allocate route-map resources.
route_map_name	The name of an existing route-map to use for filtering routes that are exported from the source VRF to the GRT.
to-all-vrfs all-routes	Exports all routes to all of the other VRF instances, except to VRFs that already have an import configured for the source (export) VRF.
to-all-vrfs route-map *route_map_name*	The name of an existing route map to use for filtering routes that are exported from the source VRF to all other VRF instances.

Defaults

- If a source VRF name is not specified with this command, routes are exported from within the context of the active VRF instance to the GRT.
- If there are no VRF instances configured on the switch, the routes are exported from the default VRF to the GRT.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable exporting of routes from the VRF to GRT.
- To leak IPv6 routes between VRF instances, IPv6 must be available in both instances. It is important to note that IPv6 route leaking is supported only in max profile VRFs.
- IPv6 route leaking supports configured tunnel routes, but 6to4 tunnel and loopback routes are not supported.
- Routes that were leaked into a VRF instance cannot be exported from that instance to another VRF.
- The route map name specified with this command must already exist in the switch configuration. See the **ip route-map** commands in the “IP Commands” chapter of this guide and the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.

- A route map created to filter exported VRF IPv6 routes can contain any of the following match and set options:
  - Match options: ipv6-address, ipv6-next-hop, tag, protocol, ipv6-interface, metric, route-type, name
  - Set options: tag, metric
- A route map with redist control of aggregate is supported when exporting IPv6 routes, but it is not supported when importing IPv6 routes.
- Only one route map per source VRF is allowed for filtering exported routes.
- Only those FDB (Forwarding Routing Database) routes that match the conditions of the route map are exported to GRT.
- Modifying a route map that is assigned to a VRF through the **ipv6 import** or **ipv6 export** command is supported.

Examples

The following commands export IPv6 routes from the current VRF routing table (or from the default VRF if there are no other VRFs configured) to the GRT:

```
-> ipv6 export route-map R1
-> ipv6 export all-routes
-> ipv6 export to-all-vrfs all-routes
-> ipv6 export to-all-vrfs route-map R2
-> no ipv6 export
```

The following commands export IPv6 routes from the “vrf2” routing table to the GRT even though the command line is operating within the context of the default VRF instance:

```
-> vrf vrf2 ipv6 export route-map R1
-> vrf vrf2 ipv6 export all-routes
-> vrf vrf2 ipv6 export to-all-vrfs all-routes
-> vrf vrf2 ipv6 export to-all-vrfs route-map R2
-> no vrf vrf2 ipv6 export
```

The following commands first change the command line context to the “vrf1” instance so that all subsequent commands export routes from “vrf1” without having to specify the VRF name with each command:

```
-> vrf vrf1
vrf1::-> ipv6 export route-map R1
vrf1::-> ipv6 export all-routes
vrf1::-> ipv6 export to-all-vrfs all-routes
vrf1::-> ipv6 export to-all-vrfs route-map R2
vrf1::-> no ipv6 export
```

Release History

Release 8.5R1; command introduced.

Related Commands

vrf	Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match protocol	Matches the protocol specified in the route map with the protocol of the route.
show ipv6 export	Displays the export route configuration details.
show ipv6 global-route-table	Displays the GRT for all the routes that are exported from the VRFs.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIprmV6ExportRouteMap
alaIprmV6ExportToAllVrfsRouteMap
```

ipv6 import

Imports VRF IPv6 routes from the GRT to the destination VRF. All routes are imported or a route map can be specified to filter imported routes.

[vrf *dest_vrf_name***] ipv6 import {vrf {***src_vrf_name* **| default} | isid** *instance_id***} {all-routes | route-map** *route_map_name***}**

[vrf *dest_vrf_name***] no ipv6 import vrf {***src_vrf_name* **| default}**

Syntax Definitions

dest_vrf_name	The name of the destination VRF instance into which routes are imported from the GRT.
src_vrf_name	The name of the source VRF instance from which routes were exported to the GRT. Routes from this instance are imported from the GRT into the specified destination VRF instance.
default	Default VRF. The routes are imported from the default VRF instance.
instance_id	An existing ISID number that identifies an SPB service in a provider backbone bridge (PBB) network. The routes for this ISID number are imported from the GRT into the current or specified VRF instance.
all-routes	Imports all routes from the source VRF instance. Imported routes are not filtered.
route_map_name	The name of an existing route map to use for filtering routes that are imported from the GRT to the destination VRF. Imported routes are filtered based on the options defined in the route map.

Defaults

If a destination VRF name is not specified with this command, routes are imported from the GRT into the context of the active VRF instance.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the IP import routes configuration for the specified VRF or ISID instance.
- To leak IPv6 routes between VRF instances, IPv6 must be available in both instances. It is important to note that IPv6 route leaking is supported only in max profile VRFs.
- IPv6 route leaking supports configured tunnel routes, but 6to4 tunnel and loopback routes are not supported.
- Routes that were leaked into a VRF instance cannot be exported from that instance to another VRF.
- The route map name specified with this command must already exist in the switch configuration. See the **ip route-map** commands in the “IP Commands” chapter of this guide and the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about

how to create a route map.

- A route map created to filter imported VRF or ISID IPv6 routes can contain any of the following match and set parameter options:
  - Match options: ipv6-address (no aggregates), ipv6-next-hop, tag, metric
  - Set options: tag, metric
- A route map with redist control of aggregate is supported when exporting IPv6 routes, but it is not supported when importing IPv6 routes.
- Only one route map per source (imported) VRF or ISID is allowed.
- Modifying a route map that is assigned to a VRF or ISID through the **ipv6 import** or **ipv6 export** command is supported.
- Leaked routes are only for forwarding. If a local route is leaked, that interface is not accessible in the importing VRF. Another switch will not be able to ping the interface in the import VRF.

Examples

```
-> ipv6 import vrf V1 route-map R2
-> ipv6 import vrf V2 all-routes
-> no ipv6 import vrf V1

-> vrf V3 ipv6 import vrf V2 route-map import-map
-> vrf V3 no ipv6 import vrf V2

-> ipv6 import isid 1500 route-map R1
-> ipv6 import isid 2000 all-routes
-> no ipv6 import isid 1500

-> vrf V4 ipv6 import isid 2500 route-map import-map
-> vrf V4 no ipv6 import isid 2500
```

Release History

Release 8.5R1; command introduced.
Release 8.5R2; **isid** parameter added.

Related Commands

vrf	Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match protocol	Matches the protocol specified in the route map with the protocol of the route.
show ipv6 import	Displays the import route configuration details.
show ipv6 global-route-table	Displays the GRT for all the routes that are exported from the VRFs.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIprmV6ImportVrfTable
   alaIprmV6ImportVrfName
   alaIprmV6ImportVrfRouteMap
   alaIprmV6ImportIsid
   alaIprmV6ImportVrfRowStatus
```

show ipv6 export

Displays the export route configuration details.

[vrf *vrf_name***] show ipv6 export**

Syntax Definitions

vrf_name	The name of an existing VRF instance.

Defaults

By default, the export route configuration for the active VRF instance is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If a VRF is specified, the export route configuration for that VRF is displayed.

Examples

```
-> show ipv6 export
Export Route Map: leak-out

-> vrf vrf1 show ipv6 export
Export Route Map: none (all-routes)

vrf2::-> show ipv6 export
Export Route Map: none (all-routes) -> To All VRFs
```

Release History

Release 8.5R1; command introduced.

Related Commands

ipv6 export	Exports IPv6 routes from the source VRF to the Global Routing Table (GRT) or to all VRF instances.

MIB Objects

```
alaIprmV6ExportRouteMap
alaIprmV6ExportToAllVrfsRouteMap
```

show ipv6 import

Displays the import route configuration details.

[vrf *vrf_name***] show ipv6 import**

Syntax Definitions

vrf_name	The name of an existing VRF instance.

Defaults

By default, the import route configuration for the active VRF instance is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If a VRF is specified, the import route configuration for that VRF is displayed.

Examples

```
-> show ipv6 import
Type  Source               RouteMap
-----+--------------------+----------------------
vrf    Customer1           leak-in
vrf    Customer2           none (all-routes)
isid   1000                isid1000-filter
```

output definitions

Type	The type of imported route (**vrf** or **isid**).
Source	The name of the VRF instance from which IPv6 routes are imported to the VRF.
RouteMap	The name of the route map filter or **none (all-routes)**.

Release History

Release 8.5R1; command introduced.
Release 8.5R2; imported ISID route entries added to the table.

Related Commands

ipv6 import	Imports VRF IPv6 routes from the GRT to the destination VRF.

MIB Objects

```
alaIprmV6ImportVrfTable
   alaIprmV6ImportVrfName
   alaIprmV6ImportIsid
   alaIprmV6ImportVrfRouteMap
   alaIprmV6ImportIsidRouteMap
   alaIprmV6ImportVrfRowStatus
```

show ipv6 global-route-table

Displays the contents of the Global Routing Table (GRT) for all the IPv6 routes that are exported from VRF or from Shortest Path Bridging service instance identifiers (ISIDs). This command is only available within the context of the default VRF instance.

show ipv6 global-route-table [export-vrf *vrf_name***]**

Syntax Definitions

vrf_name	The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

By default, exported routes are displayed for all VRF instances and ISIDs.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **export-vrf** parameter to display exported routes for a specific VRF instance.

Examples

```
-> show ipv6 global-route-table
Type   Source          Destination            Gateway               Metric  Tag
-----+--------------+---------------------+---------------------+-------+-------
 vrf  Customer2       1601::/16             1701:ffff:0001::1       1       100
 vrf  Customer2       1111::/16             1111::1                 2         5
 vrf  Customer3       2808:3456::/32        3939::2                 1         0
 isid 1000            1801::/16             2222::2                 1         2
```

output definitions

Type	The type of exported route (**vrf** or **isid**).
Source	The name of the VRF instance or the Shortest Path Bridging service instance identifier (ISID) from which IPv6 routes are exported to the GRT.
Destination	The address of the route.
Gateway	The next hop for the destination address.
Metric	The metric of the exported route.
Tag	The tag of the exported route.

Release History

Release 8.5R1; command introduced.
Release 8.5R2; exported ISID route entries added to the table.

Related Commands

ipv6 export	Configures a route map to export routes from the source VRF to Global Routing Table (GRT).
show ipv6 export	Displays the export route configuration details.

MIB Objects

```
alaGrt6RouteTable
   alaGrt6RouteDistinguisher
   alaGrt6RouteDest
   alaGrt6RouteMaskLen
   alaGrt6RouteNextHop
   alaGrt6RouteMetric
   alaGrt6RouteTag
   alaGrt6GrtVrfName
   alaGrt6RouteIsid
```

21 IPsec Commands

IPsec is a suite of protocols for securing IPv6 communications by authenticating and/or encrypting each IPv6 packet in a data stream. IPsec provides security services such as Encrypting traffic, Integrity validation, Authenticating the peers, and Anti-replay.

IPsec protocols operate at network layer using appropriate security protocols, cryptographic algorithms, and cryptographic keys. The security services are provided through use of two security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

There are two modes of IPsec operation: transport mode and tunnel mode. In transport mode, only the data you transfer (payload) in the IPv6 packet is encrypted and/or authenticated and only the payloads that are originated and destined between two intermediate systems are processed with IPsec. In tunnel mode, the entire IPv6 packet with both the data and the message headers is encrypted and/or authenticated. In tunnel mode, all the IPv6 packets that passess through the endpoints are processed by IPsec. The current implementation of IPsec supports only the transport mode.

Note. The current implementation of IPsec supports only IPv6.

The pre-configured Security Policy determines the traffic that is to be rendered with IPsec protection. A Security Association (SA) specifies the actual IPsec actions to be performed (e.g encryption using 3DES, authentication with HMAC-SHA1). A security association is bundle of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. Security Associations can be manually configured or negotiated through IKE. The current implementation of IPsec does not support the negotiation of SA through IKE and SAs need to be configured manually.

Filename: ALCATEL-IND1-IPSEC-MIB.mib
Module: alcatelIND1IPsecMIB

A summary of the available commands is listed here:

ipsec key

Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

ipsec key *name* **{sa-authentication | sa-encryption} [encrypted]** *key*

no ipsec key *name* **{sa-authentication | sa-encryption}**

Syntax Definitions

name	The name of this key (maximum 20 characters).
sa-authentication	Indicates that the key value is used for Authentication Header.
sa-encryption	Indicates that the key value is used for Encapsulated Security Payload.
encrypted	Not user configured, used only by switch in config file.
key	Specifies the key value. The key value can be either in the hexadecimal format or as a string.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The *name* parameter must be same as the name of the manually configured SA that uses this SA authentication and encryption key.
- The length of the key value must match the value that is required by the encryption or authentication algorithm that uses the key. The required key length for the supported algorithm are as follows:

algorithm	key length
3des-cbc	192 bits
aes-cbc	128, 192, or 256 bits
hmac-md5	128 bits
hmac-sha1	160 bits
aes-xcbc-mac	128

- The combination of the key's name and type must be unique.
- The **encrypted** option is used when the key commands are written to the boot.cfg or other snapshot file. This option can not be specified by the user when entering CLI commands.

Examples

```
-> ipsec key sa_md5_in sa-authentication takd03c9@skL68L%
```

Release History

Release 7.1.1; command introduced.

Related Commands

ipsec sa	Adds, modifies, or deletes a manually configured IPsec Security Association (SA).
show ipsec key	Displays the keys for the manually configured IPsec SA.

MIB Objects

```
AlaIPsecKeyTable
   alaIPsecKeyName
   alaIPsecKeyType
   alaIPsecKeyEncrypted
   alaIPsecKey
```

ipsec security-key

Sets the master security key for the switch. The master security key is used to encrypt and decrypt the configured SA keys.

ipsec security-key [*old_key***]** *new_key*

Syntax Definitions

old_key	The current master security key. The key can be specified either in the hexadecimal format or as a string.
new_key	The new key value. The key can be specified either in the hexadecimal format or as a string.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The *old_key* parameter must always be specified when you modify an existing key. Setting the key for first time does not require the *old_key*.
- If the value of the *old_key* is incorrect, the attempt to set a new key fails.
- While the SA keys can be configured without a master security key; the configured SA keys are written to the configuration file unencrypted, and a warning is logged.
- The security key must be 16 characters or 16 bytes if in hex form (32 hex digits).
- If the master security key is reset using **debug clear ipsec security-key** command, the currently configured SA keys are deleted.

Examples

```
-> ipsec security-key “old key value ab” 0xa38d901bde77af091a2485ce0a14a8cc
```

Release History

Release 7.1.1; command introduced.

Related Commands

ipsec key	Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

MIB Objects

```
AlaIPsecSecurityKeyTable
   alaIPsecSecurityKeyCurrent
   alaIPsecSecurityKeyNew
```

ipsec policy

Adds, modifies, or removes a security policy.

ipsec policy *name* **[priority** *priority***] [source {***ipv6_address***[***/prefix_length***]} [port** *port***]] [destination {***ipv6_address***[***/prefix_length***]} [port** *port***]] [protocol {any | icmp6 [type** *type***]| tcp | udp | ospf | vrrp | number** *protocol***}] [in | out] [discard | ipsec | none] [description** *description***] [admin-state {enable | disable}]**

no ipsec policy *name*

Syntax Definitions

name	The name for the policy.
priority	The priority for the policy. Values may range from 1 to 1000. The lower the value, the higher the priority.
source *ipv6_address*	Specifies the source address of the IPv6 traffic that is covered by the policy.
source */prefix_length*	Specifies the prefix length of the source address of the IPv6 traffic that is covered by the policy.
source port	Specifies the source port of the IPv6 traffic that is covered by the policy. The value 0 can be specified to match packets originated from any port.
destination *ipv6_address*	Specifies the destination address of the IPv6 traffic that is covered by the policy.
destination */prefix-length*	Specifies the prefix length of the destination address of the IPv6 traffic that is covered by the policy.
destination *port*	Specifies the destination port of the IPv6 traffic that is covered by the policy. The value 0 can be specified to match packets destined to any port.
protocol	Specifies that the particular protocol specific traffic to be covered by the policy (Refer to the table in the “Usage Guidelines“ section below for various protocol options).
in	Specifies that the policy is applied to the inbound IPv6 traffic.
out	Specifies that the policy is applied to the outbound IPv6 traffic.
discard	Specifies the policy to discard the IPv6 packet, if it matches the criteria.
ipsec	Specifies the policy to send the IPv6 packet for IPsec processing, if it matches the criteria.
none	Specifies IPsec should not process the packet.
description	The detailed description of the policy.
enable	Administratively enables the policy.
disable	Administratively disables the policy.

Defaults

parameter	default
priority	100
port	0
any | icmp6 | tcp | udp | ospf | vrrp | number	**any**
icmp6 *type*	not present
discard | ipsec | none	**ipsec**
admin-state	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- If two policies can cover the same traffic, the policy with the highest priority is applied. If two policies have the same priority, the one configured first has precedence.
- The following table lists the various **protocol** options in this command:

protocol
any
icmp6[type *type***]**
tcp
udp
ospf
vrrp
number *protocol*

The **any** option must be used to apply the policy to all protocol traffic. Otherwise, an upper-layer protocol (or protocol number) may be specified to restrict the policy to the specified protocol traffic. The optional *type* parameter of **icmp6** can also be specified to restrict the policy for certain type of ICMPv6 packets.

- If the **ipsec** option is specified this policy cannot be enabled until at least one rule has been defined. The policy rules specify that IPsec algorithms be applied to the traffic that matches the policy.

Examples

```
-> ipsec policy tcp_out source 2001:db8:3::12 destination 201:db8:4::a3e protocol
tcp out ipsec description “Outbound TCP traffic” admin-state disable
-> no ipsec policy tcp_out
```

Release History

Release 7.1.1; command introduced.

Related Commands

ipsec policy rule	Adds, modifies, or removes an IPsec rule for a security policy.
show ipsec policy	Displays information about the security policies.

MIB Objects

```
AlaIPsecSecurityPolicyTable
   alaIPsecSecurityPolicyName
   alaIPsecSecurityPolicyPriority
   alaIPsecSecurityPolicySource
   alaIPsecSecurityPolicySourceType
   alaIPsecSecurityPolicySourcePrefixLength
   alaIPsecSecurityPolicySourcePort
   alaIPsecSecurityPolicyDestination
   alaIPsecSecurityPolicyDestinationType
   alaIPsecSecurityPolicyDestinationPrefixLength
   alaIPsecSecurityPolicyDestinationPort
   alaIPsecSecurityPolicyULProtocol
   alaIPsecSecurityPolicyICMPv6Type
   alaIPsecSecurityPolicyDirection
   alaIPsecSecurityPolicyAction
   alaIPsecSecurityPolicyDescription
   alaIPsecSecurityPolicyAdminState
```

ipsec policy rule

Adds, modifies, or removes an IPsec rule for a security policy.

ipsec policy *name* **rule** *index* **[ah | esp]**

no ipsec policy *name*

Syntax Definitions

name	The name of the security policy created by using the **ipsec policy** command.
index	The index of this rule. Values may range from 1 to 10.
ah	Specifies that the rule requires the presence of an Authentication Header (AH).
esp	Specifies that the rule requires the presence of an Encrypted Security Payload header (ESP).

Defaults

N/A.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the *index* parameter to specify the order in which the multiple rules for the same security policy are applied to the original payload.

Examples

```
-> ipsec policy alucent rule 1 ah
-> no ipsec policy alucent
```

Release History

Release 7.1.1; command introduced.

Related Commands

ipsec policy	Adds, modifies, or removes a security policy.

MIB Objects

```
AlaIPsecSecurityPolicyRuleTable
   alaIPsecSecurityPolicyName
   alaIPsecSecurityPolicyRuleIndex
   alaIPsecSecurityPolicyRuleProtocol
```

ipsec sa

Adds, modifies, or deletes a manually configured IPsec Security Association (SA).

ipsec sa *name* **{esp | ah} [source** *ipv6_address* **] [destination** *ipv6_address***] [spi** *spi***] [encryption {null | 3des-cbc | aes-cbc [key-size** *key_length***]}] [authentication {none | hmac-md5 | hmac-sha1 | aes-xcbc-mac}] [description** *description***] [admin-state {enable | disable}]**

no ipsec sa *name*

Syntax Definitions

name	The name assigned to this IPsec SA.
esp	Specifies the type of security association as ESP.
ah	Specifies the type of security association as AH.
source *ipv6_address*	Specifies the source address of the IPv6 traffic that is covered by the SA.
destination *ipv6_address*	Specifies the destination address of the IPv6 traffic that is covered by the SA.
spi	The Security Parameters Index (SPI) for the SA.
encryption	Specifies the encryption algorithm to be used for traffic covered by the SA. This parameter must be used only when the SA type is ESP.
key_length	Key length for the specified encryption algorithm.
authentication	Specifies the authentication algorithm to be used for traffic covered by the SA.
description	The detailed description of the SA.
enable	Administratively enables the SA.
disable	Administratively disables the SA.

Defaults

parameter	Defaults
encryption	**none**
authentication	**none**
admin-state	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The **encryption** parameter must be specified with the **none** option, if **ESP** is being used to verify integrity only.

- If **null** is specified as the option for **encryption**, an integrity algorithm must be specified using the **authentication** parameter.
- To override a default key length in an **encryption** algorithm, the key length must be specified after the protocol name.The key length supported for various algorithm are as follows:

encryption algorithm	key length (in bits)
aes-cbc	128(default), 192, and 256

- For AH SAs, one of the authentication algorithms such as aes-xcbc-mac, hmac-md5 or hmac-sha1 must be specified.

Examples

```
-> ipsec sa esp_in_1 esp source 2001:db8:3::13d destination 2001:db8:1::24 spi
10392 encryption aes-cbc authentication hmac-sha1
-> no ipsec sa esp_in_1
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ipsec sa	Displays information about manually configured IPsec Security Associations.

MIB Objects

```
AlaIPsecSAConfigTable
   alaIPsecSAConfigName
   alaIPsecSAConfigType
   alaIPsecSAConfigSource
   alaIPsecSAConfigSourceType
   alaIPsecSAConfigDestination
   alaIPsecSAConfigDestinationType
   alaIPsecSAConfigSPI
   alaIPsecSAConfigEncryptionAlgorithm
   alaIPsecSAConfigEncryptionKeyLength
   alaIPsecSAConfigAuthenticationAlgorithm
   alaIPsecSAConfigDescription
   alaIPsecSAConfigAdminState
```

ipsec default-discard

Enable or disable the default discard policy.

ipsec default-discard admin-state {enable | disable}

Syntax Definitions

enable	Enables the default discard policy.
disable	Disables the default discard policy

Defaults

parameter	default
admin-state	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The default discard policy drops all the inbound traffic that does not match an IPsec policy.
- When incoming traffic is dropped due to the default discard policy, an SWLog informational message is logged.
- The default discard policy on its own drops all the incoming traffic destined for the switch. It is required to add appropriate higher priority policies to allow the desired traffic to be received. At a minimum, policies must be added to allow neighbor discovery traffic to be accepted.
  For example:
  -> ipsec policy ns-in priority 100 source ::/0 destination ::/0 protocol ICMP6 type 135 in none
  -> ipsec policy na-in priority 100 source ::/0 destination ::/0 protocol ICMP6 type 136 in none
- The default discard policy will be given the name **default-discard** when it is enabled. In case, the name conflicts with an existing user-defined policy, a numeric value will be appended to make the policy name unique (**default-discard-1**).
- If there is an existing user-defined policy that matches the default discard policy selectors (like source, destination, protocol, direction), then the default-discard policy cannot be enabled.
- The default discard policy is not applied to the forwarded traffic.

Examples

```
-> ipsec policy default-discard admin-state enable
-> ipsec policy default-discard admin-state disable
```

Release History

Release 8.4.1; command introduced.

Related Commands

show ipsec policy	Displays information about the security policies.

MIB Objects

```
alaIPsecDefaultDiscardPolicy
```

show ipsec policy

Displays information about the security policies.

show ipsec policy [*name***]**

Syntax Definitions

name	The policy name.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the *name* parameter to display information about a specific security policy.

Examples

```
-> show ipsec policy
Default discard policy = Enabled

Name            Priority  Source->Destination           Protocol   Direction   Action     State
--------------+--------+-----------------------------+----------+-----------+----------+--------
default-discard  1000    ::/0 -> ::/0                    any        in        discard    active
ftp-in-drop      100     ::/0->2001:db8:3::13d           TCP        in        discard    active
telnet-in-1      100     2001:db8::/48->2001:db8:1::24   TCP        in        ipsec      active
telnet-out-1     100     2001:db8:1::24->2001:db8::/48   TCP        out       ipsec       active
```

output definitions

Default discard policy	Indicates whether the default discard policy is enabled or disabled.
Name	The name of the security policy.
Priority	The priority set for the policy.
Source -> Destination	Indicates the source and destination of traffic covered by this policy.
Protocol	Indicates the protocol traffic covered by this policy. The protocol name (TCP) or protocol number (80) is displayed in this field.
Direction	Indicates whether the policy has been applied to the incoming or outgoing traffic.
Action	Indicates the action to be taken on the traffic covered by this policy.
State	Indicates the operational state of this policy.

```
-> show ipsec policy icmp_in
Policy
  Name        = icmp_in,
  Priority    = 100,
  Source      = 100::1/0,
```

```
  Destination = 100::2/0,
  Protocol    = ICMP6,
  Direction   = in,
  Action      = none,
  State       = active
```

output definitions

Name	The name of the security policy.
Priority	The priority set for the policy.
Source	Indicates the source of the traffic covered by this policy.
Destination	Indicates the destination of the traffic covered by this policy.
Protocol	Indicates the protocol traffic covered by this policy. The protocol name (TCP) or protocol number (80) is displayed in this field.
Direction	Indicates whether the policy has been applied to the incoming or outgoing traffic.
Action	Indicates the action to be taken on the traffic covered by this policy.
State	Indicates the operational state of this policy.

Release History

Release 7.1.1; command introduced.
Release 8.4.1; **default discard policy** field added.

Related Commands

ipsec policy	Adds, modifies, or removes a security policy.
ipsec default-discard	Enable or disable the default discard policy.

MIB Objects

```
AlaIPsecSecurityPolicyTable
   alaIPsecSecurityPolicyName
   alaIPsecSecurityPolicySource
   alaIPsecSecurityPolicySourceType
   alaIPsecSecurityPolicySourcePrefixLength
   alaIPsecSecurityPolicySourcePort
   alaIPsecSecurityPolicyDestination
   alaIPsecSecurityPolicyDestinationType
   alaIPsecSecurityPolicyDestinationPrefixLength
   alaIPsecSecurityPolicyDestinationPort
   alaIPsecSecurityPolicyProtocol
   alaIPsecSecurityPolicyDirection
   alaIPsecSecurityPolicyAction
   alaIPsecSecurityPolicyOperationalState
   alaIPsecSecurityPolicyRuleIndex
   alaIPsecSecurityPolicyRuleProtocol
   alaIPsecSecurityPolicyDescription
```

show ipsec sa

Displays information about manually configured IPsec Security Associations.

show ipsec sa [*name* **| esp | ah]**

Syntax Definitions

name	The name of the Security Association.
esp	Restricts the display to ESP type SAs.
ah	Restricts the display to AH type SAs.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the *name* parameter to display the information about a specific SA.
- Use esp or ah option to display the information about their respective type SAs.

Examples

```
-> show ipsec sa
Name           Type  Source-> Destination[SPI]           State   Encryption
Authentication
--------------+----+-----------------------------------+--------+----------------
telnet-in-esp  ESP  2001:db8::/49->2001:db8:1::24        active   aes-cbc(128)
hmac-sha1
telnet-out-esp ESP 2001:db8:1::24->2001:db8::/48         active   aes-cbc(128)
hmac-sha1
```

output definitions

Name	The SA name.
Type	The SA type: AH or ESP.
Source -> Destination [SPI]	The traffic source, traffic destination, and SPI for this SA.
State	The operational state of this SA.
Encryption	The encryption algorithm used for this SA.
Authentication	The authentication algorithm in use for this SA.

```
-> show ipsec sa telnet-in-esp

Name           = telnet-in-esp
Type           = ESP
Source         = 2001:db8::/48
Destination    = 2001:db8:1::24
SPI            = 8920
Encryption     = aes-cbc(128)
Authentication = hmac-sha1

State          = active
Description:
  Security association for traffic from 2001:db8::/48 to
  2001:db8:1::24.
```

output definitions

Name	The SA name.
Type	The SA type: AH or ESP.
Source	The traffic source for this SA.
Destination	The traffic destination for this SA.
SPI	The SA's SPI.
Encryption	The encryption algorithm used for this SA.
Authentication	The authentication algorithm used for this SA.
State	The operational state of this SA.
Description	The SA's description.

Release History

Release 7.1.1; command introduced.

Related Commands

ipsec sa	Adds, modifies, or deletes a manually configured IPsec Security Association (SA).

MIB Objects

```
AlaIPsecSAConfigTable
   alaIPsecSAConfigName
   alaIPsecSAConfigType
   alaIPsecSAConfigSource
   alaIPsecSAConfigSourceType
   alaIPsecSAConfigDestination
   alaIPsecSAConfigDestinationType
   alaIPsecSAConfigSPI
   alaIPsecSAConfigOperationalState
   alaIPsecSAConfigEncryptionAlgorithm
   alaIPsecSAConfigEncryptionKeyLength
   alaIPsecSAConfigAuthenticationAlgorithm
   alaIPsecSAConfigAuthenticationKeyLength
   alaIPsecSAConfigDescription
```

show ipsec key

Displays the keys for the manually configured IPsec SA.

show ipsec key [sa-encryption | sa-authentication]

Syntax Definitions

sa-encryption	Displays the encryption keys.
sa-authentication	Displays the authentication keys.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The key values are not be displayed due to security reasons.

Examples

```
-> show ipsec key sa-encryption
Encryption Keys
Name                 Length (bits)
--------------------+-------------
sa_1                            192
sa_2                            160
sa_3                             64

-> show ipsec key sa-authentication
Authentication Keys
Name                 Length (bits)
--------------------+-------------
sa_1                            128
sa_5                            160
```

output definitions

Name	The name of the SA for which the key is used.
Length	The length of the key in bits.

Release History

Release 7.1.1; command introduced.

Related Commands

ipsec key	Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

MIB Objects

```
AlaIPsecKeyTable
   alaIPsecKeyName
   alaIPsecKey
```

show ipsec ipv6 statistics

Displays IPsec statistics.

show ipsec ipv6 statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ipsec ipv6 statistics

Inbound:
  Discarded                  = 2787
  Policy violation          = 0
  Authentication Failure     = 0
  No SA found                = 0
Outbound:
  Discarded                  = 5135
  No SA found                = 19
```

output definitions

Discarded	The number of incoming packets discarded because they matched a discard policy.
Policy violation	The number of incoming packets that don’t have the IPsec protection required by a security policy.
Authentication Failure	Authentication of a packet failed.
No SA found	No SA found matching the information present in a packet.

Release History

Release 7.1.1; command introduced.

Related Commands

show ipsec policy	Displays information about the security policies.
show ipsec sa	Displays information about manually configured IPsec Security Associations.

MIB Objects

```
AlaIPsecStatisticsTable
   alaIPsecStatisticsInDiscarded
   alaIPsecStatisticsInPolicyViolation
   alaIPsecStatisticsInAHAuthenticationFail
   alaIPsecStatisticsInNoSA
   alaIPsecStatisticsOutDiscarded
   alaIPsecStatisticsOutPolicyViolation
   alaIPsecStatisticsOutNoSA
```

22 RIP Commands

Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) that uses hop count as its routing metric. RIP-enabled switches update neighboring switches by transmitting a copy of their own routing table. The RIP routing table always uses the most efficient route to a destination, that is, the route with the fewest hops and longest matching prefix.

The switch supports RIP version 1 (RIPv1), RIP version 2 (RIPv2), and RIP next generation (RIPng). It also supports simple and MD5 authentication, on an interface basis, for RIPv2.

The RIP commands comply with the following RFCs: RFC1058, RFC2453, RFC1722, RFC1723, RFC1724, and RFC2080.

MIB information for the RIP commands is as follows:

Filename: ALCATEL-IND1-VIRTUALROUTER-MIB.mib
Module: alcatelIND1VirtualRouterMIB

Filename: RIPv2-MIB.mib
Module: rip2

Filename: ALCATEL-IND1-RIP-MIB.mib
Module: alcatelIND1RIPMIB

Filename: ALCATEL-IND1-RIPNG-MIB.mib
Module: alcatelIND1RipngMIB

A summary of the available commands is listed here:

ip load rip	**ipv6 load rip**
ip rip admin-state	**ipv6 rip admin-state**
ip rip interface	**ipv6 rip invalid-timer**
ip rip interface admin-state	**ipv6 rip garbage-timer**
ip rip interface metric	**ipv6 rip holddown-timer**
ip rip interface send-version	**ipv6 rip jitter**
ip rip interface recv-version	**ipv6 rip route-tag**
ip rip interface ingress-filter	**ipv6 rip update-interval**
ip rip interface egress-filter	**ipv6 rip triggered-sends**
ip rip force-holddowntimer	**ipv6 rip interface**
ip rip host-route	**ipv6 rip interface metric**
ip rip route-tag	**ipv6 rip interface recv-status**
ip rip interface auth-type	**ipv6 rip interface send-status**
ip rip interface auth-key	**ipv6 rip interface horizon**
ip rip update-interval	**show ipv6 rip**
ip rip invalid-timer	**show ipv6 rip interface**
ip rip garbage-timer	**show ipv6 rip peer**
ip rip holddown-timer	**show ipv6 rip routes**
show ip rip	
show ip rip routes	
show ip rip interface	
show ip rip peer	

ip load rip

Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.

ip load rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- In simple networks where only IP forwarding is required, you may not want to use RIP. If you are not using RIP, it is best not to load it to save switch resources.
- To remove RIP from switch memory, you must manually edit the **boot.cfg** file. The **boot.cfg** file is an ASCII text-based file that controls many of the switch parameters. Open the file and delete all references to RIP. You must reboot the switch when this is complete.
- Use the **ip rip admin-state** command to enable RIP on the switch.

Examples

```
-> ip load rip
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip admin-state	Enables/disables RIP routing on the switch.
show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaVrConfigTable
   alaVrConfigRipStatus
```

ip rip admin-state

Enables/disables RIP on the switch. RIP performs well in small networks. By default, RIP packets are broadcast every 30 seconds, even if no change has occurred anywhere in a route or service. Depending on the size and speed of the network, these periodic broadcasts can consume a significant amount of bandwidth.

ip rip admin-state {enable | disable}

Syntax Definitions

enable	Enables RIP routing on the switch.
disable	Disables RIP routing on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- RIP must be loaded on the switch (**ip load rip**) to enable RIP on the switch.
- A RIP network can be no more than 15 hops (end-to-end). If there is a 16th hop, that network is identified as infinity and the packet is discarded.

Examples

```
-> ip rip admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip load rip	Loads RIP into the switch memory.
show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipProtoStatus
```

ip rip interface

Creates/deletes a RIP interface. Routing is enabled on a VLAN when you create a router interface. However, to enable RIP routing, you must also configure and enable a RIP routing interface on the VLAN's IP router interface.

ip rip interface {*interface_name***}**

no ip rip interface {*interface_name***}**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- By default, a RIP interface is created in the disabled state. To enable RIP routing on the interface, you must enable the interface by using the **ip rip interface admin-state** command.
- You can create a RIP interface even if an IP router interface has not been configured. However, RIP will not function unless an IP router interface is configured with the RIP interface.
- For more information on VLANs and router ports, see Chapter 5, "VLAN Management Commands".

Examples

```
-> ip rip interface rip-1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip interface	Creates a VLAN router interface.
ip load rip	Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.
ip rip admin-state	Enables/disables RIP routing on the switch.
ip rip interface admin-state	Enables/disables a RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfStatus
```

ip rip interface admin-state

Enables and disables a RIP interface. By default, a RIP interface is created in the disabled state. After creating a RIP interface, you must use this command to enable the interface.

ip rip interface {*interface_name***} admin-state {enable | disable}**

Syntax Definitions

interface_name	The name of the interface.
enable	Administratively enables RIP on the interface.
disable	Administratively disables RIP on the interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You must first create a RIP interface by using the **ip rip interface** command before enabling the interface.
- You can create a RIP interface even if an IP router interface has not been configured. However, RIP will not function unless an IP router interface is configured with the RIP interface.
- For more information on VLANs and router ports, see Chapter 5, “VLAN Management Commands”.

Examples

```
-> ip rip interface rip-1 admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip interface	Creates a VLAN router interface.
ip load rip	Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.
ip rip admin-state	Enables/disables RIP routing on the switch.
ip rip interface	Creates/deletes a RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfStatus
```

ip rip interface metric

Configures the RIP metric or cost for a specified interface. You can set priorities for routes generated by a switch by assigning a metric value to routes generated by that switch's RIP interface. For example, routes generated by a neighboring switch may have a hop count of 1. However, you can lower the priority of routes generated by that switch by increasing the metric value for routes generated by the RIP interface.

ip rip interface {*interface_name***} metric** *value*

Syntax Definitions

interface_name	The name of the interface.
value	Metric value. Valid range is 1–15.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When you configure a metric for a RIP interface, this metric cost is added to the metric of the incoming route.

Examples

```
-> ip rip interface rip-1 metric 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface	Enables/disables RIP on a specific interface.
show ip rip peer	Displays active RIP neighbors (peers). An active peer is a switch that has sent a RIP packet within the last 180 seconds.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfDefaultMetric
```

ip rip interface send-version

Configures the send option for a RIP interface. This defines the type(s) of RIP packets that the interface will send.

ip rip interface {*interface_name***} send-version {none | v1 | v1compatible | v2}**

Syntax Definitions

interface_name	The name of the interface.
none	RIP packets will not be sent by the interface.
v1	Only RIPv1 packets will be sent by the interface.
v1compatible	Only RIPv2 broadcast packets (not multicast) will be sent by the interface.
v2	Only RIPv2 packets will be sent by the interface.

Defaults

parameter	default
none | v1 | v2 | v1compatible	**v2**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Using this command will override RIP default behavior.
- Other devices must be able to interpret the information provided by this command or there will not be proper routing information exchanged between the switch and other devices on the network.

Examples

```
-> ip rip interface rip-1 send-version v1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface recv-version	Configures the receive option for a RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfSend
```

ip rip interface recv-version

Configures the receive option for a RIP interface. This defines the type(s) of RIP packets that the interface will accept.

ip rip interface {*interface_name***} recv-version {v1 | v2 | both | none}**

Syntax Definitions

interface_name	The name of the interface.
v1	Only RIPv1 packets will be received by the interface.
v2	Only RIPv2 packets will be received by the interface.
both	Both RIPv1 and RIPv2 packets will be received by the interface.
none	Interface ignores any RIP packets received.

Defaults

parameter	default
v1 | v2 | both | none	**both**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Using this command will override RIP default behavior.
- Other devices must be able to interpret the information provided by this command or there will not be proper routing information exchanged between the switch and other devices on the network.

Examples

```
-> ip rip interface rip-1 recv-version both
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface send-version	Configures the send option for a RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfReceive
```

ip rip interface ingress-filter

Assigns an ingress route map filter to the specified RIP interface. Received route advertisements are compared against ingress filters. When a prefix matches the corresponding filter, that prefix is accepted on the interface. When a prefix does not match the filter, the prefix is dropped as if it was never received.

ip rip interface {*interface_name***} ingress-filter {***filter_name***}**

Syntax Definitions

interface_name	The name of an existing RIP interface.
filter_name	The name of an existing route-map filter.

Defaults

By default, no such filter is associated with the RIP interface.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- One route-map filter is configurable in each direction (ingress/egress) for each RIP interface.
- Configuring multiple filters in the same direction for a single RIP interface is not supported.

Examples

```
-> ip route-map ripfilter1 action permit
-> ip route-map ripfilter1 match ip-address 202.5.0.0/16 deny
-> ip rip interface vlan-100 Ingress-filter RipFilter1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface egress-filter	Assigns an egress route map filter to a RIP interface.
show ip rip interface	Displays RIP interface status and configuration.

MIB Objects

N/A

ip rip interface egress-filter

Assigns an egress route map filter to the specified RIP interface. Outbound route advertisements are compared against egress filters. When a prefix matches the corresponding filter, that prefix is sent on the interface. When a prefix does not match the filter, the prefix is dropped as if it did not exist in the RIP RIB.

ip rip interface {*interface_name***} egress-filter {***filter_name***}**

Syntax Definitions

interface_name	The name of an existing RIP interface.
filter_name	The name of an existing route-map filter.

Defaults

By default, no such filter is associated with the RIP interface.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- One route-map filter is configurable in each direction (ingress/egress) for each RIP interface.
- Configuring multiple filters in the same direction for a single RIP interface is not supported.

Examples

```
-> ip route-map ripfilter1 action permit
-> ip route-map ripfilter1 match ip-address 202.5.0.0/16 deny
-> ip rip interface vlan-100 egress-filter RipFilter1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

iip rip interface egress-filter	Assigns an ingress route map filter to a RIP interface.
show ip rip interface	Displays RIP interface status and configuration.

MIB Objects

N/A

ip rip force-holddowntimer

Configures the forced hold-down timer value, in seconds, that defines an amount of time during which routing information regarding better paths is suppressed. A route enters into a forced hold-down state when an update packet is received that indicates the route is unreachable and when this timer is set to a non-zero value. After this timer has expired and if the value is less than 120 seconds, the route enters a hold-down state for the rest of the period until the remainder of the 120 seconds has also expired. During this time the switch will accept any advertisements for better paths that are received.

ip rip force-holddowntimer *seconds*

Syntax Definitions

seconds	The forced hold-down time interval. The valid range is 0–120 seconds.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The forced hold-down timer is not the same as the RIP hold-down timer. The forced hold-down timer defines a separate interval that overlaps the hold-down state. During the forced hold-down timer interval, the switch will not accept *better* routes from other gateways.
- The forced hold-down time interval can become a subset of the hold-down timer (120 seconds) by using this command to set a value less than 120.
- To allow the routing switch to use better routes advertised during the entire hold-down time period, leave the forced hold-down timer set to the default value.

Examples

```
-> ip rip force-holddowntimer 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (for example, forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipForceHolddownTimer
```

ip rip host-route

Specifies whether or not RIP can add host routes (routes with a 32-bit mask) to the RIP table.

ip rip host-route

no ip rip host-route

Syntax Definitions

N/A

Defaults

The default is to enable a default host route.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to prevent RIP from adding host routes to the RIP table.
- When enabled, RIPv1 will interpret an incoming route announcement that contains any 1 bit in the host portion of the IP address as a host route, implying a mask of 255.255.255.255.

Examples

```
-> ip rip host-route
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip rip routes	Displays the RIP Routing Database.

MIB Objects

```
alaProtocolRip
   alaRipHostRouteSupport
```

ip rip route-tag

Configures the route tag value for RIP routes generated by the switch.

ip rip route-tag *value*

Syntax Definitions

value	Route tag value. Valid range is 0–2147483647.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Only RIPv2 supports route tags.

Examples

```
-> ip rip route-tag 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaRipRedistRouteTag
```

ip rip interface auth-type

Configures the type of authentication that will be used for the RIP interface. By default, there is no authentication used for RIP. However, you can configure a password for a RIP interface. To configure a password, you must first select the authentication type (simple or MD5), then configure a password.

ip rip interface {*interface_name***} auth-type {none | simple | md5}**

Syntax Definitions

interface_name	The name of the interface.
none	No authentication will be used.
simple	Simple authentication will be used.
md5	MD5 authentication will be used.

Defaults

parameter	default
none | simple | md5	**none**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Regardless of which authentication type is used (simple or MD5), both switches on either end of a link must share the same password.

Examples

```
-> ip rip interface rip-1 auth-type none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface auth-key	Configures the text string that will be used as the password for the RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfAuthType
```

ip rip interface auth-key

Configures the text string that will be used as the password for the RIP interface. If you configure simple or MD5 authentication, you must configure a text string that will be used as the password for the RIP interface.

ip rip interface {*interface_name***} auth-key** *string*

Syntax Definitions

interface_name	The name of the interface.
string	16-byte text string.

Defaults

The default authentication string is a null string.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Regardless of which authentication type is used (simple or MD5), both switches on either end of a link must share the same password.

Examples

```
-> ip rip interface rip-1 auth-key nms
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface auth-type	Configures the type of authentication that will be used for the RIP interface.

MIB Objects

```
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfAuthKey
```

ip rip update-interval

Configures the time interval during which RIP routing updates are sent out.

ip rip update-interval *seconds*

Syntax Definitions

seconds	The RIP routing update interval, in seconds. The valid range is 1–120.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The update interval value must be less than or equal to one-third the invalid interval value.

Examples

```
-> ip rip update-interval 45
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipUpdateInterval
```

ip rip invalid-timer

Configures the RIP invalid timer value that defines the time interval during which a route will remain active in Routing Information Base (RIB) before moving to the invalid state.

ip rip invalid-timer *seconds*

Syntax Definition

seconds	The RIP invalid timer value, in seconds. The valid range is 3–360.

Defaults

parameter	default
seconds	180

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The invalid time interval value must be three times the update interval value.

Examples

```
-> ip rip invalid-timer 270
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipInvalidTimer
```

ip rip garbage-timer

Configures the RIP garbage timer value that defines the time interval, which must elapse before an expired route is removed from the RIB.

ip rip garbage-timer *seconds*

Syntax Definition

seconds	The RIP garbage timer value, in seconds. The valid range is 0–180.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

During the RIP garbage interval, the router advertises the route with a metric of INFINITY (i.e., 16 hops).

Examples

```
-> ip rip garbage-timer 180
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipGarbageTimer
```

ip rip holddown-timer

Configures the RIP hold-down timer value that defines the time interval during which a route remains in the hold-down state.

ip rip holddown-timer *seconds*

Syntax Definition

seconds	The hold-down time interval, in seconds. The valid range is 0–120.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When RIP detects a route with higher metric than the route in the RIB, the route with the higher metric goes into the hold-down state. The route updates with a metric of INFINITY are rejected.

Examples

```
-> ip rip holddown-timer 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip rip	Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

```
alaProtocolRip
   alaRipHolddownTimer
```

show ip rip

Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

show ip rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip rip

Status                    = Enabled
Number of routes          = 9
Host Route Support        = Enabled
Route Tag                 = 42
Update interval           = 30
Invalid interval          = 180
Garbage interval          = 120
Holddown interval         = 0
Forced Hold-Down Timer    = 0
```

output definitions

Status	RIP status (**Enabled** or **Disabled**).
Number of routes	Number of network routes in the RIP routing table.
Host Route Support	Host route status (**Enabled** or **Disabled**). Indicates whether or not RIP can add host routes (routes with a 32-bit mask) to the RIP table.
Route Tag	Route tag value for RIP routes generated by the switch. Valid values are 0–2147483647.
Update interval	The RIP routing update interval, in seconds.
Invalid interval	The RIP invalid timer value, in seconds.
Garbage interval	The RIP garbage timer value, in seconds.
Holddown interval	The hold-down time interval, in seconds.
Forced Hold-Down Timer	The forced hold-down time interval, in seconds.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip admin-state	Enables/disables RIP routing on the switch.
ip rip force-holddowntimer	Configures the interval during which a RIP route remains in the forced hold-down state.
ip rip update-interval	Configures the time interval during which RIP routing updates are sent out.
ip rip invalid-timer	Configures the RIP invalid timer value that defines the time interval during which a route will remain active in Routing Information Base (RIB) before moving to the invalid state.
ip rip garbage-timer	Configures the RIP garbage timer value that defines the time interval, which must elapse before an expired route is removed from the RIB.
ip rip holddown-timer	Configures the RIP hold-down timer value that defines the time interval during which a route remains in the hold down state.

MIB Objects

```
alaProtocolRip
   alaRipProtoStatus
   alaRipRouteNumber
   alaRipHostRouteSupport
   alaRipRedistRouteTag
   alaRipUpdateInterval
   alaRipInvalidTimer
   alaRipGarbageTimer
   alaRipHolddownTimer
   alaRipForceHolddownTimer
```

show ip rip routes

Displays the RIP routing database. The routing database contains all of the routes learned through RIP.

show ip rip routes [*ip_address ip_mask***]**

Syntax Definitions

ip_address	32-bit IP address.
ip_mask	The mask corresponding to the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To view all RIP routes, enter the basic command syntax (**show ip rip routes**). To view a specific route, enter the destination IP address and mask.

Examples

```
-> show ip rip routes

Legends: State: A = Active, H = Holddown, G = Garbage
Destination        Gateway          State Metric Proto
-----------------+----------------+----+------+------
2.0.0.0/8          +5.0.0.14          A    2      Rip
                    4.0.0.7           A    3      Rip
4.0.0.0/8          +5.0.0.14          A    3      Rip
                    2.0.0.14          A    3      Rip
5.0.0.0/8          +2.0.0.14          A    2      Rip
                    4.0.0.7           A    3      Rip
10.0.0.0/8         +4.0.0.7           A    2      Rip
                    5.0.0.14          A    2      Rip
                    2.0.0.14          A    2      Rip
22.0.0.0/8         +5.0.0.14          A    2      Rip
                    2.0.0.14          A    2      Rip
                    4.0.0.7           A    3      Rip
128.251.40.0/24    +4.0.0.7           A    2      Rip
                    5.0.0.14          A    3      Rip
                    2.0.0.14          A    3      Rip
150.0.0.0/24       +4.0.0.7           A    2      Rip
                    5.0.0.14          A    2      Rip
                    2.0.0.14          A    2      Rip
152.0.0.0/24       +4.0.0.7           A    2      Rip
                    5.0.0.14          A    3      Rip
```

output definitions

Destination	Destination network IP address.
Gateway	The Gateway IP address (switch from which the destination address was learned).
State	The associated state of the route, which can be **A** (**Active**), **H** (**Holddown**), or **G** (**Garbage**).
Metric	Metric associated with this network. Generally, this is the RIP hop count (the number of hops from this switch to the destination switch).
Proto	The type of route (**Local**, **Rip**, or **Redist**).

```
-> show ip rip routes 2.0.0.0 255.0.0.0

Destination             = 2.0.0.0,
Mask length             = 8,
Gateway(1)              = 5.0.0.14,
  Protocol              = Rip,
  Out Interface         = intf5,
  Metric                = 2,
  Status                = Installed,
  State                 = Active,
  Age                   = 19s,
  Tag                   = 0,
Gateway(2)              = 4.0.0.7,
  Protocol              = Rip,
  Out Interface         = intf4,
  Metric                = 3,
  Status                = Not Installed,
  State                 = Active,
  Age                   = 12s,
  Tag                   = 0,
```

output definitions

Destination	Destination network IP address.
Mask length	Length of the destination network IP subnet mask.
Gateway	The Gateway IP address (switch from which the destination address was learned).
Protocol	The type of the route (**Local**, **Rip**, or **Redist**).
Out Interface	The RIP interface through which the next hop is reached.
Metric	Metric associated with this network. Generally, this is the RIP hop count (the number of hops from this switch to the destination switch).
Status	The RIP interface status (Installed or Not Installed).
State	The associated state of the route (**Active**, **Holddown**, or **Garbage**).
Age	The age of the route in seconds (the number of seconds since this route was last updated or otherwise determined to be correct).
Tag	The associated route tag.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip host-route	Enables/disables a host route to an individual host on a network.

MIB Objects

```
alaRipEcmpRouteTable
   alaRipEcmpRouteDest
   alaRipEcmpRouteMask
   alaRipEcmpRouteNextHop
   alaRipEcmpRouteType
   alaRipEcmpMetric
   alaRipEcmpStatus
   alaRipEcmpAge
   alaRipEcmpTag
   alaRipEcmpRouteState
   alaRipEcmpRouteStatus
```

show ip rip interface

Displays RIP interface status and configuration.

show ip rip interface [*interface_name***]**

Syntax Definitions

interface_name	The interface name.

Defaults

By default, the status and configuration for all RIP interfaces is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enter an interface name to view detailed information for a specific interface.

Examples

```
-> show ip rip interface
       Interface      Domain   Domain    Intf Admin   IP Intf      Updates
         Name         Name       ID       status      status     sent/recv(bad)
--------------------+--------+--------+-----------+-----------+---------------
v12                  Vlan     12       disabled    enabled     0/0(0)
s101                 Service  101      enabled     enabled     0/0(0)
t1                   Tunnel    NA      disabled    disabled    0/0(0)

-> show ip rip interface v12
Interface IP Name                      = v12,
Interface IP Address                   = 12.1.1.1,
Domain Name                            = Vlan,
Domain ID                              = 12,
Interface Admin status                 = disabled,
IP Interface Status                    = enabled,
Interface Config Ingress Route Map Name = ,
Interface Config Egress Route Map Name  = ,
Interface Config AuthType              = None,
Interface Config AuthKey Length        = 0,
Interface Config Send-Version          = v2,
Interface Config Receive-Version       = both,
Interface Config Default Metric        = 1,
Received Packets                       = 0,
Received Bad Packets                   = 0,
Received Bad Routes                    = 0,
Sent Updates                           = 0

san@jackson show ip rip interface s101
Interface IP Name                      = s101,
Interface IP Address                   = 13.1.1.1,
Domain Name                            = Service,
```

```
Domain ID                               = 101,
Interface Admin status                  = enabled,
IP Interface Status                     = enabled,
Interface Config Ingress Route Map Name = ,
Interface Config Egress Route Map Name  = ,
Interface Config AuthType               = None,
Interface Config AuthKey Length         = 0,
Interface Config Send-Version           = v2,
Interface Config Receive-Version        = both,
Interface Config Default Metric         = 1,
Received Packets                        = 77564,
Received Bad Packets                    = 0,
Received Bad Routes                     = 0,
Sent Updates                            = 77557

-> show ip rip interface t1
Interface IP Name                       = t1,
Interface IP Address                    = 10.1.1.2,
Domain Name                             = Tunnel,
Domain ID                               = NA,
Interface Admin status                  = enabled,
IP Interface Status                     = enabled,
Interface Config Ingress Route Map Name = ,
Interface Config Egress Route Map Name  = ,
Interface Config AuthType               = None,
Interface Config AuthKey Length         = 0,
Interface Config Send-Version           = v2,
Interface Config Receive-Version        = both,
Interface Config Default Metric         = 1,
Received Packets                        = 0,
Received Bad Packets                    = 0,
Received Bad Routes                     = 0,
Sent Updates                            = 0
```

output definitions

Interface IP Name	The IP Interface name.
Interface IP Address	Interface IP address.
Domain Name	The domain on which the IP interface was configured (**VLAN**, **Service**, or **Tunnel**).
Domain ID	The VLAN ID or service ID on which the IP interface was configured. This field displays “NA” for IP tunnels.
Interface Admin Status	The RIP administrative status (enabled/disabled).
IP Interface Status	Interface status (enabled /disabled).
Interface Config Ingress Route Map Name	The name of the route map applied to filter RIP routing updates received on the interface.
Interface Config Egress Route Map Name	The name of the route map applied to filter RIP routing updates sent on the interface.
Interface Config AuthType	The type of authentication that will be used for the RIP interface (None or Simple).
Interface Config AuthKey Length	The authentication key length used for the RIP interface.

output definitions (continued)

Interface Config Send-Version	Interface send option (none, v1, v2, and v1 compatible).
Interface Config Receive-Version	Interface receive option (none, v1, v2, and both).
Interface Config Default Metric	Default redistribution metric.
Received Packets	Number of packets received on the interface.
Received Bad Packets	Number of bad packets received and discarded. Normally this value is zero (0).
Received Bad Routes	Number of bad routes received and discarded. Normally this value is zero (0).
Sent Updates	Number of RIP routing table updates sent.

Release History

Release 7.1.1; command was introduced.
Release 8.6R2; “Domain Name” and “Domain ID” fields added.

Related Commands

ip rip interface	Enables/disables RIP for a specific interface.

MIB Objects

```
alaProtocolRip
   alaRipProtoStatus
alaRip2IfConfAugTable
   alaRip2IfConfEncryptKey
   alaRip2IfIpConfStatus
   alaRip2IfRecvPkts
   alaRip2IfConfName
   alaRip2IfConfType
   alaRip2IfConfPtoPPeer
   alaRip2IfConfIngressFilterRouteMapName
   alaRip2IfConfEgressFilterRouteMapName
   alaRip2IfIfIndex
rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfAuthType
   rip2IfConfAuthKey
   rip2IfConfSend
   rip2IfConfReceive
   rip2IfConfDefaultMetric
rip2IfStatTable
   rip2IfStatRcvBadPackets
   rip2IfStatRcvBadRoutes
   rip2IfStatSentUpdates
```

show ip rip peer

Displays active RIP neighbors (peers). An active peer is a switch that has sent a RIP packet within the last 180 seconds. If a peer does not send a RIP packet (request or response) within 180 seconds, it is aged out and will not be displayed.

show ip rip peer [*ip_address*]

Syntax Definitions

ip_address	32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip rip peer

                Total   Bad     Bad             Secs since
    IP Address   Recvd  Packets Routes Version  last update
----------------+------+-------+------+-------+-----------
  100.10.10.1      1      0       0      2       3
```

output definitions

IP Address	Peer IP address.
Total recvd	Total number of RIP packets received from the peer.
Bad Packets	Number of bad packets received from peer.
Bad Routes	Number of bad routes received from peer.
Version	Peer's RIP version as seen on the last packet received.
Secs since last update	Number of seconds since the last packet was received from the peer.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip rip interface	Displays the RIP interface status and configuration.

MIB Objects

```
rip2PeerTable
   rip2PeerAddress
   rip2PeerDomain
   rip2PeerLastUpdate
   rip2PeerVersion
   rip2PeerRcvBadPackets
   rip2PeerRcvBadRoutes
```

ipv6 load rip

Loads RIPng into memory. When the switch is initially configured, you must load RIPng into memory to enable RIPng routing.

ipv6 load rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- RIPng will support a maximum of 1,000 routes.
- RIPng will support a maximum of 20 interfaces.
- Use the **ipv6 rip admin-state** command to enable RIPng on the switch.

Examples

```
-> ipv6 load rip
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip admin-state	Enables/disables RIPng routing on the switch.
show ipv6 rip	Displays RIPng status and general configuration parameters.

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPRipngStatus
```

ipv6 rip admin-state

Enables or disables RIPng on the switch.

ipv6 rip admin-state {enable | disable}

Syntax Definitions

enable	Enables RIPng.
disable	Disables RIPng.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

RIPng must be loaded on the switch (**ip load rip**) to enable RIP on the switch.

Examples

```
-> ipv6 rip admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip load rip	Loads RIPng into memory.
show ipv6 rip	Displays RIPng status and general configuration parameters.

MIB Objects

```
alaProtocolripng
   alaRipngProtoStatus
```

ipv6 rip invalid-timer

Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.

ipv6 rip invalid-timer *seconds*

Syntax Definitions

seconds	Time, in seconds, that a route will remain in an “Active” state. Valid range is 1 - 300.

Defaults

parameter	default
seconds	180

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This timer is reset each time a routing update is received.

Examples

```
-> ipv6 rip invalid-timer 300
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip garbage-timer	Configures the RIPng garbage timer value.
ipv6 rip holddown-timer	Configures the amount of time a route is placed in a holddown state.

MIB Objects

```
alaProtocolripng
   alaRipngInvalidTimer
```

ipv6 rip garbage-timer

Configures the RIPng garbage timer value. When a route in the RIB exceeds the configured Invalid Timer Value, the route is moved to a “Garbage” state in the the RIB. The garbage timer is the length of time a route will stay in this state before it is flushed from the RIB.

ipv6 rip garbage-timer *seconds*

Syntax Definitions

seconds	Time, in seconds, that a route will remain in the RIPng Routing Table before it is flushed from the RIB. Valid range is 0 - 180.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **ipv6 rip invalid-timer** command to set the Invalid Timer Value.

Examples

```
-> ipv6 rip garbage-timer 180
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip invalid-timer	Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.
ipv6 rip holddown-timer	Configures the amount of time a route is placed in a holddown state.

MIB Objects

```
alaProtocolripng
   alaRipngGarbageTimer
```

ipv6 rip holddown-timer

Configures the amount of time a route is placed in a holddown state. Whenever a route is seen from the same gateway with a higher metric than the route in RIB, the route goes into holddown. This excludes route updates with an INFINITY metric.

ipv6 rip holddown-timer *seconds*

Syntax Definitions

seconds	Time, in seconds, that a route will remain in a holddown state. Valid range is 0 - 120.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

While in holddown, the route continues being announced as usual and used in RIB. This interval is used to control route flap dampening.

Examples

```
-> ipv6 rip holddown-timer 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip invalid-timer	Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.
ipv6 rip garbage-timer	Configures the RIPng garbage timer value.

MIB Objects

```
alaProtocolripng
   alaRipngHolddownTimer
```

ipv6 rip jitter

Configures an offset value for RIPng updates. This is the maximum (positive or negative) value that can be used to offset the update interval. For example, with an update interval of 30 seconds, and a jitter value of 5 seconds, the RIPng update packet would be sent somewhere (random) between 25 and 35 seconds from the previous update.

ipv6 rip jitter *value*

Syntax Definitions

value	Time, in seconds, that a routing update is offset. Valid range is 0 to one-half the updated interval value (e.g., if the updated interval is 30, the range would be 0 - 300).

Defaults

parameter	default
value	5

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

As you increase the number of RIPng interfaces/peers, it is recommended that you increase the Jitter value to reduce the number of RIPng updates being sent over the network.

Examples

```
-> ipv6 rip jitter 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip update-interval	Configures the RIPng update interval.
show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngJitter
```

ipv6 rip route-tag

Configures the route tag value for RIP routes generated by the switch.

ipv6 rip route-tag *value*

Syntax Definitions

value	Route tag value. Valid range is 0 – 65535.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This value does not apply to routes learned from other routers. For these routes, the route tag propagates with the route.

Examples

```
-> ipv6 rip route-tag 30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngRouteTag
```

ipv6 rip update-interval

Configures the RIPng update interval. This is the interval, in seconds, that RIPng routing updates will be sent out.

ipv6 rip update-interval *seconds*

Syntax Definitions

seconds	Interval, in seconds, that RIPng routing updates are sent out. Valid range is 0–120.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command, along with the **ipv6 rip jitter** command to configure RIPng updates.

Examples

```
-> ipv6 rip update-interval 30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip jitter	Configures an offset value for RIPng updates.
show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaRipng
   alaRipngUpdateInterval
```

ipv6 rip triggered-sends

Configures the behavior of triggered updates.

ipv6 rip triggered-sends {all | updated-only | none}

Syntax Definitions

all	All RIPng routes are added to any triggered updates.
updated-only	Only route changes that are causing the triggered update are included in the update packets.
none	RIPng routes are not added to triggered updates.

Defaults

parameter	default
all | updated-only | none	**updated-only**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If set to **all**, all routes are sent in the update, not just route changes, which increases RIPng traffic on the network.
- If set to **none**, no triggered updates are sent, which can cause delays in network convergence.

Examples

```
-> ipv6 rip triggered-sends none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngTriggeredSends
```

ipv6 rip interface

Creates or deletes a RIPng interface.

ipv6 rip interface *if_name*

no ipv6 rip interface *if_name*

Syntax Definitions

if_name	IPv6 interface name.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- By default, a RIPng interface is created in the enabled state.
- Routing is enabled on a VLAN when you create a router port. However, to enable RIPng routing, you must also configure and enable a RIPng routing interface on the VLAN's IP router port. For more information on VLANs and router ports, see Chapter 5, "VLAN Management Commands".
- RIPng will support a maximum of 20 interfaces.

Examples

```
-> ipv6 rip interface Test_Lab
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 load rip	Loads RIPng into memory.
ipv6 rip admin-state	Enables or disables RIPng on the switch.
ipv6 rip interface recv-status	Configures IPv6 RIPng interface “Receive” status. When this status is set to "enable", packets can be received on this interface.
ipv6 rip interface send-status	Configures IPv6 RIPng interface “Send” status. When this status is set to "enable", packets can be sent on this interface.
show ipv6 rip interface	Displays information for all or specified RIPng interfaces.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceStatus
```

ipv6 rip interface metric

Configures the RIPng metric or cost for a specified interface. You can set priorities for routes generated by a switch by assigning a metric value to routes generated by that switch's RIPng interface. For example, routes generated by a neighboring switch may have a hop count of 1. However, you can lower the priority of routes generated by that switch by increasing the metric value for routes generated by the RIPng interface.

ipv6 rip interface *if_name* **metric** *value*

Syntax Definitions

if_name	IPv6 interface name.
value	Metric value. Valid range is 1 - 15.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When you configure a metric for a RIPng interface, this metric cost is added to the metric of the incoming route.

Examples

```
-> ipv6 rip Test_Lab metric 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip interface	Creates or deletes a RIPng interface.
show ipv6 rip interface	Displays information for all or specified RIPng interfaces.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceMetric
```

ipv6 rip interface recv-status

Configures IPv6 RIPng interface “Receive” status. When this status is set to "enable", packets can be received on this interface. When it is set to "disable", packets will not be received on this interface.

ipv6 rip interface *if_name* **recv-status {enable | disable}**

Syntax Definitions

if_name	IPv6 interface name.
enable	Enables the “Receive” status for the specified interface.
disable	Disables the “Receive” status for the specified interface.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

RIPng must be loaded (**ip load rip**) and enabled (**ipv6 rip admin-state**) on the switch to send or receive packets on the interface.

Examples

```
-> ipv6 rip interface Test_Lab recv-status disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 load rip	Loads RIPng into memory.
ipv6 rip admin-state	Enables/disables RIPng on the switch.
ipv6 rip interface send-status	Configures IPv6 RIPng interface “Send” status.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceRecvStatus
```

ipv6 rip interface send-status

Configures IPv6 RIPng interface “Send” status. When this status is enabled, packets can be sent from this interface. When it is disabled, packets will not be sent from this interface.

ipv6 rip interface *if_name* **send-status {enable | disable}**

Syntax Definitions

if_name	IPv6 interface name.
enable	Enables the “Send” status for the specified interface.
disable	Disables the “Send” status for the specified interface.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

RIPng must be loaded (**ip load rip**) and enabled (**ipv6 rip admin-state**)on the switch to send or receive packets on the interface.

Examples

```
-> ipv6 rip interface Test_Lab send-status enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 load rip	Loads RIPng into memory.
ipv6 rip admin-state	Enables/disables RIPng on the switch.
ipv6 rip interface recv-status	Configures IPv6 RIPng interface “Receive” status.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceSendStatus
```

ipv6 rip interface horizon

Configures the routing loop prevention mechanisms.

ipv6 rip interface *if_name* **horizon {none | split-only | poison}**

Syntax Definitions

if_name	IPv6 interface name.
none	Disables loop prevention mechanisms.
split-only	Enables split-horizon, without poison-reverse.
poison	Enables split-horizon with poison-reverse.

Defaults

parameter	default
none | split-only | poison	**poison**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If set to **none** the route is not sent back to the peer.
- If set to **split-only**, the route received from the peer is sent back with an increased metric.
- If set to **poison** the route received from the peer is sent back with an “infinity” metric.

Examples

```
-> ipv6 rip interface Test_Lab none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 rip interface	Displays information for all or specified RIPng interfaces.
show ipv6 rip routes	Displays all or a specific set of routes in the RIPng Routing Table.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceHorizon
```

show ipv6 rip

Displays the RIPng status and general configuration parameters.

show ipv6 rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 rip

Status              = Enabled,
Number of routes    = 10,
Route tag           = 0,
Update interval     = 30,
Invalid interval    = 180,
Garbage interval    = 120,
Holddown interval   = 0,
Jitter interval     = 5,
Triggered Updates   = All Routes,
```

output definitions

Status	RIPng protocol status (enabled or disabled).
Number of routes	Number of RIPng routes in Forwarding Information Base (FIB).
Route tag	Route tag value for RIP routes generated by the switch. Default is 0.
Invalid interval	Invalid Timer setting, in seconds.
Garbage interval	Garbage Timer setting, in seconds.
Holddown interval	Holddown Timer setting, in seconds.
Jitter interval	Jitter setting.
Triggered updates	Triggered Updates setting (All Routes, Updated Routes, and None).

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip admin-state	Enables or disables RIPng routing on the switch.
ipv6 rip route-tag	Configures the route tag value for RIP routes generated by the switch.
ipv6 rip update-interval	Configures the Interval, in seconds, so that RIPng routing updates are sent out.
ipv6 rip invalid-timer	Configures the amount of time a route remains active in RIB before being moved to the "garbage" state.
ipv6 rip invalid-timer	Configures the RIPng garbage timer value. Routes move into the garbage collection state because the timer expired or a route update with an INFINITY metric was received.
ipv6 rip holddown-timer	Configures the amount of time a route is placed in a holddown state.
ipv6 rip jitter	Configures an offset value for RIPng updates. This is the maximum (positive or negative) value that can be used to offset the update interval.
ipv6 rip triggered-sends	Configures the behavior of triggered updates.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceStatus
   alaRipngRouteTag
   laRipngInvalidTimer
   alaRipngGarbageTimer
   alaRipngHolddownTimer
   alaRipngJitter
   alaRipngTriggeredSends
```

show ipv6 rip interface

Displays information for all or specified RIPng interfaces.

show ipv6 rip interface [*if_name*]

Syntax Definitions

if_name	IPv6 interface name.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If an interface name is not specified, all IPv6 RIP interfaces are displayed.

Examples

```
-> show ipv6 rip interface

    Interface                        Packets
       Name           Status     Recvd   Sent     Metric
--------------------+----------+---------+--------+---------
Test_Lab             Active     12986     12544    1
Test_Lab_2           Active     12556     12552    1


-> show ipv6 rip interface if3

Name                           = Test_Lab,
IPv6 interface index           = 3,
Interface status               = Active,
Next Update                    = 27 secs,
Horizon Mode                   = Split and Poison-reverse,
MTU size                       = 1500,
Metric                         = 1,
Send status                    = Enabled,
Receive status                 = Enabled,
Packets received               = 12986,
Packets sent                   = 12544,
```

output definitions

Interface name	Interface name.
IPv6 interface index	IPv6 index of this interface.
Status	Interface status (Active/Inactive).
Packets Recvd	Number of packets received by the interface.

output definitions (continued)

Packets Sent	Number of packets sent by the interface.
Metric	RIPng metric (cost) configured for the interface.
IPv6 interface index	IPv6 interface index number.
Interface status	Interface status (Active/Inactive).
Next update	Seconds remaining until the next update on this interface.
Horizon mode	Interface Horizon Mode (routing loop prevention mechanisms). Displayed modes are none/split-only/poison-reverse.
MTU size	Maximum transmission size for RIPng packets on the interface.
Send status	Interface “Send” status. When this status is set to "enable", packets can be sent from this interface. When it is set to "disable", packets will not be sent from this interface.
Receive status	Interface “Receive” status. When this status is set to "enable", packets can be received by this interface. When it is set to "disable", packets cannot be received by this interface.
Packets received	Number of packets received by the interface.
Packets sent	Number of packets sent by the interface.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip interface	IPv6 interface name.
ipv6 rip admin-state	Enables or disables RIPng routing on the switch.
ipv6 rip interface recv-status	Configures the interface “Receive” status. When this status is set to "enable", packets can be received by this interface. When it is set to "disable", packets cannot be received by this interface.
ipv6 rip interface send-status	Configures the interface “Send” status. When this status is set to "enable", packets can be sent from this interface. When it is set to "disable", packets will not be sent from this interface.
ipv6 rip interface metric	Configures the RIPng metric (cost) for the interface.
ipv6 rip interface horizon	Configures the interface Horizon Mode (routing loop prevention mechanisms).
show ipv6 rip	Displays RIPng status and general configuration parameters (e.g., force holddown timer).

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceEntry
   alaRipngInterfaceStatus
   alaRipngInterfacePacketsRcvd
   alaRipngInterfacePacketsSent
   alaRipngInterfaceMetric
   alaRipngInterfaceIndex
   alaRipngInterfaceNextUpdate
   alaRipngInterfaceHorizon
   alaRipngInterfaceMTU
   alaRipngInterfaceSendStatus
   alaRipngInterfaceRecvStatus
```

show ipv6 rip peer

Displays a summary of the observed RIPng peers, or specific information about a peer when a peer address is provided.

show ipv6 rip peer [*ipv6_addresss*]

Syntax Definitions

ipv6_addresss	IPv6 address of the peer.

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If you do not specify a peer, all IPv6 RIP peers are displayed.

Examples

```
-> show ipv6 peer
                              Seen on       Packets   Last
Address                       Interface     Recv      Update
------------------------------+-------------+--------+----------
fe80::200:39ff:fe1f:710c      vlan172       23       20
fe80::2d0:95ff:fe12:da40      bkbone20      33       2
fe80::2d0:95ff:fe12:da40      vlan150       26       25
fe80::2d0:95ff:fe6a:5d41      nssa23        20       25

-> show ipv6 rip peer fe80::2d0:95ff:fe12:da40

Peer#1 address          = fe80::2d0:95ff:fe12:da40,
Seen on interface       = bkbone20,
Last Update             = 8 secs,
Received packets        = 33,
Received bad packets    = 0
Received routes         = 5,
Received bad routes     = 0

Peer#2 address          = fe80::2d0:95ff:fe12:da40,
Seen on interface       = vlan150,
Last Update             = 1 secs,
Received packets        = 27,
Received bad packets    = 0
Received routes         = 2,
Received bad routes     = 0
```

output definitions

Address	IPv6 address of the peer.
Seen on Interface	Interface used to reach the peer.
Packets Recvd	Number of packets received from the peer.
Last Update	Number of seconds since the last update was received from the peer.
Peer address	Peer IPv6 address.
Received packets	Number of packets received from the peer.
Received bad packets	Number of bad packets received from the peer.
Received routes	Number of RIPng routes received from the peer.
Received bad routes	Number of bad RIPng routes received from the peer.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 rip interface	Displays all or specified RIPng interface status.
show ipv6 rip routes	Displays all or a specific set of routes in RIPng Routing Table.

MIB Objects

```
alaRipngPeerTable
   alaRipngPeerEntry
   alaRipngPeerAddress
   alaRipngPeerIndex
   alaRipngPeerLastUpdate
   alaRipngPeerNumUpdates
   alaRipngPeerBadPackets
   alaRipngPeerNumRoutes
   alaRipngPeerBadRoutes
```

show ipv6 rip routes

Displays all or a specific set of routes in RIPng Routing Table.

show ipv6 rip routes [dest *ipv6_prefix/prefix_length* **| gateway** *ipv6_addr* **| detail** *ipv6 prefix/ prefix_length***]**

Syntax Definitions

dest	Displays all routes whose destination matches the IPv6 prefix/prefix length.
gateway	Displays all routes whose gateway matches the specified IPv6 address.
detail	Displays detailed information about a single route matching the specified destination.
ipv6_prefix/prefix length	IPv6 address and prefix/prefix length.
ipv6_addr	IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If none of the optional parameters are entered with this command, all IPv6 RIP routes are displayed.

Examples

```
-> show ipv6 rip routes

Legends: State: A = Active, H = Holddown, G = Garbage
Destination     Gateway                      State    Metric Proto
---------------+----------------------------+-------+------+------
100::1/128      +fe80::200:39ff:fe1f:710c     A       2      Rip
100::100:1/128  +fe80::200:39ff:fe1f:710c     A       2      Rip
400::/100       +fe80::2d0:95ff:fe12:e050     A       1      Local
900::/100       +fe80::2d0:95ff:fe12:e050     A       1      Local
8900::/100      +fe80::2d0:95ff:fe12:da40     A       2      Rip
9800::/100      +fe80::2d0:95ff:fe12:da40     A       2      Rip
9900::/100      +fe80::2d0:95ff:fe12:e050     A       1      Local
```

```
-> show ipv6 rip routes detail 9900::/100

Destination     = 9900::,
Mask length     = 100,
Gateway(1)      = fe80::2d0:95ff:fe12:e050,
Protocol        = Local,
Out Interface   = nssa23,
Metric          = 1,
Status          = Installed,
State           = Active,
Age             = 10544s,
Tag             = 0,
Gateway(2)      = fe80::2d0:95ff:fe12:da40,
Protocol        = Rip,
Out Interface   = bkbone20,
Metric          = 2,
Status          = Not Installed,
State           = Active,
Age             = 15s,
Tag             = 0,
```

output definitions

Destination	IPv6 address/address length of the destination.
Gateway	IPv6 gateway used to reach the destination.
State	Route status (Active/Inactive).
Metric	Routing metric for this route.
Protocol	Protocol used to learn the route.
Mask Length	Prefix Length.
Out Interface	The interface used to reach the destination.
Status	Route status (Active/Inactive).
Age	The number of seconds since the route was last updated.
Tag	The route tag value for the route.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip interface	Creates/deletes a RIPng interface.
ipv6 rip interface metric	Configures the RIPng metric or cost for a specified interface.
show ipv6 rip interface	Displays all or specified RIPng interface status.

MIB Objects

```
alaRipngRouteTable
   alaRipngRouteEntry
   alaRipngRoutePrefixLen
   alaRipngRouteNextHop
   alaRipngRouteType
   alaRipngRouteAge
   alaRipngRouteTag
   alaRipngRouteStatus
   alaRipngRouteMetric
```

23 BFD Commands

Bidirectional Forwarding Detection (BFD) is a hello protocol, which can be configured to interact with routing protocols for the detection of path failures and can reduce the convergence time in a network. BFD is supported with the BGP, IS-IS, OSPF, PIM, VRRP, and Static Routes.

When BFD is configured and enabled, BFD sessions are created and timers are negotiated between BFD neighbors. If a system does not receive a BFD control packet within the negotiated time interval, the neighbor system is considered down. Rapid failure detection notices are then sent to the routing protocol, which initiates a routing protocol recalculation. This process can reduce the time of convergence in a network.

This implementation of BFD supports an Asynchronous control packet mode or an Asynchronous Echo function. Demand mode is not supported.

- When the Asynchronous control packet mode is activated, BFD neighbors periodically send BFD control packets to each other. A time interval for transmitting and receiving such packets is negotiated between the two BFD systems. If a neighboring system fails to receive a number of control packets continuously over a specific period of time, the session is considered down and BFD informs the appropriate routing protocol.
- The Asynchronous Echo function is used to verify the forwarding path between neighboring BFD systems. When active, a BFD system transmits Echo packets only (no control packets are sent) to a BFD neighbor, which then sends the packets back to the originating system along the forwarding path. If no Echo packets are received back from the BFD neighbor within a configured Echo time interval, the session is considered down.

MIB information for the BFD commands is as follows:

Filename: ALCATEL-IND1-BFD-MIB.mib
Module: alcatelIND1BfdMIB

A summary of the available commands is listed here:

Global BFD commands	**ip bfd admin-state** **ip bfd transmit** **ip bfd receive** **ip bfd multiplier** **ip bfd echo-interval** **show ip bfd** **show ip|ipv6 bfd sessions** **show ip|ipv6 bfd sessions statistics**
BFD Interface commands	**ip|ipv6 bfd interface** **ip|ipv6 bfd interface admin-state** **ip|ipv6 bfd interface transmit** **ip|ipv6 bfd interface receive** **ip|ipv6 bfd interface multiplier** **ip|ipv6 bfd interface echo-interval** **show ip|ipv6 bfd interfaces**

ip bfd admin-state

Enables or disables the global BFD protocol status for the switch.

ip bfd admin-state {enable | disable}

Syntax Definitions

enable	Enables BFD.
disable	Disables BFD.

Defaults

By default, BFD is disabled for the switch.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Disabling BFD does not remove the existing BFD configuration from the switch.
- When BFD is disabled, all BFD functionality is disabled for the switch, but configuring BFD is still allowed.
- Configuring BFD global parameters is not allowed when BFD is enabled for the switch.

Examples

```
-> ip bfd admin-state enable
-> ip bfd admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bfd	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalAdminStatus
```

ip bfd transmit

Configures the global transmit time interval for BFD control packets. This command specifies the minimum amount of time BFD waits between each transmission of control packets.

ip bfd transmit *transmit_interval*

Syntax Definitions

transmit_interval	The transmit time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
transmit_interval	300 milliseconds

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The transmit time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd transmit** command does not override the value set for the interface using the **ip bfd interface transmit** command.
- The global transmit time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd transmit 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip|ipv6 bfd interface transmit	Configures the transmit time interval for a specific BFD interface.
show ip bfd	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalTxInterval
```

ip bfd receive

Configures the global receive time interval for BFD control packets. This command specifies the minimum amount of time BFD waits to receive control packets before determining there is a problem.

ip bfd receive *receive_interval*

Syntax Definitions

receive_interval	The receive time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
receive_interval	300 milliseconds

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The minimum receive time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd receive** command does not override the value set for the interface using the **ip bfd interface receive** command.
- The global receive time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd receive 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip|ipv6 bfd interface receive	Configures the receive time interval for a specific BFD interface.
show ip bfd	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalRxInterval
```

ip bfd multiplier

Configures the global BFD detection time multiplier. This command specifies a number that is used to calculate the BFD detection time used in the asynchronous mode. The detection time value that is specified determines how long to wait before declaring that the BFD session is down.

ip bfd multiplier *num*

Syntax Definitions

num	The detection time multiplier number. The valid range is 3–255.

Defaults

By default, the multiplier value is set to 3.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The global detection time multiplier is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd multiplier** command does not override the value set for the interface using the **ip bfd interface multiplier** command.
- The global detection time multiplier serves as the default multiplier value for a BFD interface. The default multiplier value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd multiplier 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip|ipv6 bfd interface multiplier	Configures the detection time multiplier for a BFD interface.
show ip bfd	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalDetectMult
```

ip bfd echo-interval

Configures the global BFD echo packet time interval. The echo function is available with the asynchronous mode. Echo packets are transmitted to BFD peers to see if they loop back to the peer from which they originated.

ip bfd echo-interval *echo_interval*

Syntax Definitions

echo_interval	The echo time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
echo_interval	300 milliseconds

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The echo packet time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd echo-interval** command does not override the value set for the interface using the **ip bfd interface echo-interval** command.
- The global echo packet time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd echo-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip|ipv6 bfd interface echo-interval	Configures the echo packet time interval for a BFD interface.
show ip bfd	Displays the BFD global status and general configuration parameters.

MIB Objects

```
alaBfdGlobalEchoRxInterval
```

ip|ipv6 bfd interface

Configures an IPv4 or IPv6 BFD interface.

{ip | ipv6} bfd interface *if_name*

no {ip | ipv6} bfd interface *if_name*

Syntax Definitions

if_name	The name of an existing IPv4 or IPv6 interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a BFD interface.
- The interface name must be an existing IPv4 or IPv6 interface name that is configured with an IPv4or IPv6 address.

Examples

```
-> ip bfd interface bfd-vlan-101
-> no ip bfd interface bfd-vlan-101

-> ipv6 bfd interface bfd-vlan-201
-> no ipv6 bfd interface bfd-vlan-201
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip|ipv6 bfd interface admin-state	Configures the administrative status of an IPv4 or IPv6 BFD interface.
show ip|ipv6 bfd interfaces	Displays the status and statistics of a BFD interface.
show ip|ipv6 bfd sessions	Displays the status and statistics of the BFD sessions.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfIndex
   alaBfdIntfRowStatus
```

ip|ipv6 bfd interface admin-state

Enables or disables the administrative status of an IPv4 or IPv6 BFD interface.

{ip | ipv6} bfd interface *if_name* **admin-state {enable | disable}**

Syntax Definitions

if_name	The name of an existing IPv4 or IPv6 BFD interface.
enable	Enables the BFD interface.
disable	Disables the BFD interface.

Defaults

By default, a BFD interface is disabled when it is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD interface must be enabled to participate in the BFD protocol.

Examples

```
-> ip bfd interface bfd-vlan-101 admin-state enable
-> ip bfd interface bfd-vlan-101 admin-state disable

-> ipv6 bfd interface bfd-vlan-201 admin-state enable
-> ipv6 bfd interface bfd-vlan-201 admin-state disable
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip|ipv6 bfd interface	Creates an IPv4 or IPv6 BFD interface.
show ip|ipv6 bfd interfaces	Displays the status and statistics of a BFD interface.
show ip|ipv6 bfd sessions	Displays the status and statistics of BFD sessions.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfAdminStatus
```

ip|ipv6 bfd interface transmit

Configures the transmit time interval for an IPv4 or IPv6 BFD interface. This command specifies the minimum amount of time BFD waits between each transmission of control packets from the interface.

{ip | ipv6} bfd interface *if_name* **transmit** *transmit_interval*

Syntax Definitions

if_name	The name of an existing IPv4 or IPv6 BFD interface.
transmit_interval	The transmit time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
transmit_interval	300 milliseconds

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The global transmit time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface transmit time interval using the **ip bfd interface transmit** or **ipv6 bfd interface transmit** command does not change the global value configured with the **ip bfd transmit** command.

Examples

```
-> ip bfd interface bfd-vlan-101 transmit 500

-> ipv6 bfd interface bfd-vlan-201 transmit 500
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip|ipv6 bfd interface	Creates an IPv4 or IPv6 BFD interface.
ip bfd transmit	Configures a global BFD transmit time interval.
show ip|ipv6 bfd interfaces	Displays the status and statistics of a BFD interface.
show ip|ipv6 bfd sessions	Displays the status and statistics of the BFD sessions.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfDesiredMinTxInterval
```

ip|ipv6 bfd interface receive

Configures the receive time interval for an IPv4 or IPv6 BFD interface. This command specifies the minimum amount of time BFD waits to receive control packets on the interface before determining there is a problem.

{ip | ipv6} bfd interface *if_name* **receive** *receive_interval*

Syntax Definitions

if_name	The name of an existing IPv4 or IPv6 BFD interface.
receive_interval	The receive time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
receive_interval	300 milliseconds

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The global receive time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface transmit time interval using the **ip bfd interface receive** or **ipv6 bfd interface receive** command does not change the global value configured with the **ip bfd receive** command.

Examples

```
-> ip bfd interface bfd-vlan-101 receive 500

-> ipv6 bfd interface bfd-vlan-201 receive 500
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip|ipv6 bfd interface	Creates an IPv4 or IPv6 BFD interface.
ip bfd receive	Configures a global BFD receive time interval.
show ip|ipv6 bfd interfaces	Displays the BFD interface configuration table.
show ip|ipv6 bfd sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
   alaBfdReqMinRxInterval
```

ip|ipv6 bfd interface multiplier

Configures the detection time multiplier for an IPv4 or IPv6 BFD interface. This command specifies a number that is used to calculate the BFD detection time used in the asynchronous mode. When an interface stops receiving packets from a neighbor, the interface uses the detection time value to determine how long to wait before declaring that the BFD session is down.

{ip | ipv6} bfd interface *if_name* **multiplier** *num*

Syntax Definitions

if_name	The name of an existing IPv4 or IPv6 BFD interface.
num	The detection time multiplier number. The valid range is 3–255.

Defaults

By default, the multiplier value is set to 3.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The detection time between neighbors is calculated by multiplying the negotiated transmit time interval by the detection time multiplier.

Examples

```
-> ip bfd interface bfd-vlan-101 multiplier 5

-> ipv6 bfd interface bfd-vlan-201 multiplier 5
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip|ipv6 bfd interface	Creates an IPv4 or IPv6 BFD interface.
show ip|ipv6 bfd interfaces	Displays the BFD interface configuration table.
show ip|ipv6 bfd sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfDetectMult
```

ip|ipv6 bfd interface echo-interval

Configures the echo time interval for an IPv4 or IPv6 BFD interface. The echo function is available with the asynchronous mode. Echo packets are transmitted to BFD peers to see if they loop back to the peer from which they originated.

{ip | ipv6} bfd interface *if_name* **echo-interval** *echo_interval*

Syntax Definitions

if_name	The name of an existing IPv4 or IPv6 BFD interface.
echo_interval	The echo time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
echo_interval	300 milliseconds

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The global echo time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface echo time interval using the **ip bfd interface echo-interval** or **ipv6 bfd interface echo-interval** command does not change the global value configured with the **ip bfd echo-interval** command.

Examples

```
-> ip bfd interface bfd-vlan-101 echo-interval 500

-> ip bfd interface bfd-vlan-201 echo-interval 500
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip|ipv6 bfd interface	Creates an IPv4 or IPv6 BFD interface.
ip bfd echo-interval	Configures a global BFD echo time interval.
show ip|ipv6 bfd interfaces	Displays the BFD interface configuration table.
show ip|ipv6 bfd sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfReqMinEchoRxInterval
```

show ip bfd

Displays the global BFD configuration table.

show ip bfd

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip bfd
BFD Version Number              = 1,
Admin Status                    = Enabled,
Desired Tranmit Interval        = 300,
Minimum Receive Interval        = 300,
Detection Time Multiplier       = 3,
Minimum Echo Receive Interval   = 300,
Applications Registered         = STATIC-ROUTING OSPF
```

output definitions

BFD Version Number	Refers to BFD version.
Admin Status	Refers to BFD global admin status.
Desired Transmit Interval	Refers to BFD global Tx interval.
Minimum Receive Interval	Refers to BFD global Rx interval.
Detection Time Multiplier	Refers to the BFD Detection Time multiplier number.
Minimum Echo Receive Interval	Refers to BFD echo Rx interval.
Applications Registered	Refers to applications registered to BFD.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd admin-state	Configures BFD at global level.
ip|ipv6 bfd interface	Configures BFD at interface level.

MIB Objects

```
alaBfdIntfTable
   alaBfdGlobalVersionNumber
   alaBfdGlobalAdminStatus
   alaBfdGlobalTxInterval
   alaBfdGlobalRxInterval
   alaBfdGlobalDetectMult
   alaBfdGlobalEchoRxInterval
   alaBfdGlobalProtocolApps
```

show ip|ipv6 bfd interfaces

Displays the BFD interface configuration table.

show {ip | ipv6} bfd interfaces [*if_name***]**

Syntax Definitions

if_name	The name of the IPv4 or IPv6 BFD interface.

Defaults

By default, the configuration for all IPv4 or IPv6 BFD interfaces is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Enter an interface name to display information for a specific BFD interface.

Examples

```
-> show ip bfd interfaces
Interface  Admin    Tx        Min Rx   Min EchoRx Detect     OperStatus
Name       Status   Interval  Interval Interval   Multiplier
---------+--------+---------+---------+----------+----------+----------
bfd-intf1  enabled   300      300       300         3         UP
bfd-intf2  enabled   300      300       300         3         UP

-> show ip bfd interfaces bfd-intf1
Interface Name                   = bfd-intf1,
Interface IP Address             = 100.1.1.1,
Admin Status                     = Enabled,
Desired Transmit Interval        = 300,
Minimum Receive Interval         = 300,
Detection Time Multiplier        = 3,
Minimum Echo Receive Interval    = 300,
Authentication Present           = No,
Oper Status                      = UP

-> show ipv6 bfd interfaces
    Interface          Admin         Tx      Min Rx    Min EchoRx Detect  Oper
      Name             Status     Interval  Interval   Interval    Mult  Status
--------------------+----------+----------+----------+----------+------+------
bfd-intf3            disabled    300        300        300        3      DOWN

-> show ipv6 bfd interfaces bfd-intf3
Interface Name                   = bfd-intf3
Interface IP Address             = fe80::2efa:a2ff:fe13:e402,
Admin Status                     = Disabled,
Desired Transmit Interval        = 300,
Minimum Receive Interval         = 300,
Detection Time Multiplier        = 3,
```

```
Minimum Echo Receive Interval    = 300,
Authentication Present           = No,
Oper Status                      = DOWN
```

output definitions

Interface Name	Refers to BFD Interface name.
Interface IP Address	Refers to the IPv4 or IPv6 network address assigned to the BFD interface.
Admin status	Refers to BFD interface admin status.
Desired Transmit Interval	Refers to BFD interface Tx interval.
Minimum Receive Interval	Refers to BFD interface Rx interval.
Detection Time Multiplier	Refers to BFD interface Detection Time Multiplier.
Minimum Echo Receive Interval	Refers to BFD interface echo Rx interval.
Authentication Present	Refers to availability of BFD message authentication on the BFD interface.
Oper Status	Refers to BFD interface operational status.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip bfd admin-state	Configures BFD at global level.
ip|ipv6 bfd interface	Configures BFD at interface level.

MIB Objects

```
alaBfdIntfTable
   alaBfdIntfIfName
   alaBfdIntfAddr
   alabfdIntfAdminStatus
   alaBfdIntfDesiredMinTxInterval
   alaBfdIntfReqMinRxInterval
   alaBfdIntfDetectMult
   alaBfdIntfReqMinEchoRxInterval
   alaBfdIntfAuthPresFlag
   alaBfdIntfOperStatus
```

show ip|ipv6 bfd sessions

Displays the IPv4 or IPv6 BFD sessions for the switch.

show {ip | ipv6} bfd sessions [*session_num*] **[slot** *chassis/slot***]**

Syntax Definitions

session_num	The BFD session number. Valid range is 1–1024.
chassis	The chassis identifier.
slot	The current slot position used by the switch.

Defaults

By default, all IPv4 or IPv6 BFD sessions are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Specify a session number to display information for an individual BFD session.

Examples

```
-> show ip bfd sessions
Legends: Neg.     = Negotiated
         Discr    = Discriminator
         Intvl    = Interval (in milliseconds)
 Local Interface    Neighbor               State   Remote  Neg. Rx Neg. Tx EchoRx
 Discr   Name       Address                        Discr   Intvl   Intvl   Intvl
------+---------+------------------------+-------+-------+-------+-------+--------
 1       one      100.1.1.10                UP      0       0       0       ECHO
 2       one      101.1.1.11                UP      10      300     300     ASYNC

-> show ip bfd sessions slot 1
Legends: Neg.     = Negotiated
         Discr    = Discriminator
         Intvl    = Interval (in milliseconds)
 Local Interface    Neighbor               State   Remote  Neg. Rx Neg. Tx EchoRx
 Discr   Name       Address                        Discr   Intvl   Intvl   Intvl
------+---------+------------------------+-------+-------+-------+-------+--------
1        one      100.1.1.10                UP      0       0       0       300

-> show ip bfd sessions 1
Local discriminator             = 1,
Neighbor IP Address             = 100.1.1.10,
Requested Session Type          = ECHO,
Interface IP Address            = 100.1.1.1,
Source UDP Port                 = 49152,
State                           = UP,
Session Operating Mode          = ECHO only,
Remote discriminator            = 0,
```

```
Negotiated Tx interval          = 0,
Negotiated Rx interval          = 0,
Echo Rx interval                = 300,
Multiplier                      = 3,
Applications Registered:        = STATIC-ROUTING

-> show ipv6 bfd sessions
Legends: Neg.     = Negotiated
         Discr    = Discriminator
         Intvl    = Interval (in milliseconds)
 Local Interface    Neighbor               State   Remote  Neg. Rx Neg. Tx EchoRx
 Discr   Name       Address                        Discr   Intvl   Intvl   Intvl
------+---------+------------------------+-------+-------+-------+-------+--------
1      bfd-intf3 fe80::2efa:a2ff:fe13:e402  UP      0       0       0       300

-> show ipv6 bfd sessions 1
Local discriminator             = 1,
Neighbor IP Address             = fe80::2efa:a2ff:fe13:e402,
Requested Session Type          = ECHO,
Interface IP Address            = fe80::2efa:a2ff:fe13:e403,
Source UDP Port                 = 49152,
State                           = UP,
Session Operating Mode          = ECHO only,
Remote discriminator            = 0,
Negotiated Tx interval          = 0,
Negotiated Rx interval          = 0,
Echo Rx interval                = 300,
Multiplier                      = 3,
Applications Registered:        = STATIC-ROUTING
```

output definitions

Local discriminator	The local discriminator.
Neighbor IP address	The IPv4 or IPv6 address of the BFD neighbor.
Requested Session Type	The bit map of the session type that is requested.
Interface IP address	The IPv4 or IPv6 address of the outgoing BFD interface for this session.
Source UDP Port	The unique source UDP port used to send BFD packets for this session.
State	The state of the BFD session.
Session Operating Mode	The current operating mode of the BFD session.
Remote discriminator	The remote discriminator.
Negotiated Tx interval	The negotiated transmit interval.
Negotiated Rx interval	The negotiated receive interval.
Echo Rx interval	The Echo packet receive interval.
Detection Time Multiplier	The BFD Detection Time multiplier number.
Applications Registered	The bit map object of applications that are registered with this BFD session.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip bfd admin-state	Configures BFD at global level.
ip|ipv6 bfd interface	Configures BFD at interface level.
show ip|ipv6 bfd sessions statistics	Displays the statistics for all BFD sessions.

MIB Objects

```
alaBfdSessTable
   alaBfdSessDiscriminator
   alaBfdSessNeighborAddr
   alaBfdSessSessionType
   alaBfdSessIfIndex
   alaBfdSessUdpPort
   alaBfdSessState
   alaBfdSessOperMode
   alaBfdSessDiscriminator
   alaBfdSessNegotiatedTxInterval
   alaBfdSessNegotiatedRxInterval
   alaBfdSessEchoRxInterval
   alaBfdSessDetectMult
   alaBfdSessProtocolApps
```

show ip|ipv6 bfd sessions statistics

Displays the statistics for IPv4 or IPv6 BFD sessions.

show {ip | ipv6} bfd sessions statistics [*session_num***]**

Syntax Definitions

session_num	The BFD session number. Valid range is 1–1024.

Defaults

By default, statistics for all IPv4 or IPv6 sessions are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Specify a BFD session number to display statistics for an individual session.

Examples

```
-> show ip bfd sessions statistics
Legends:
 noDiag     =  noDiagnostic(0)           ctlDetExp = controlDetectionTimeExpired(1)
 echFail    =  echoFunctionFailed(2)     nbrDwn    = neighborSignaledSessionDown(3)
 fwdPlRst   =  forwardingPlaneReset(4)   pthDwn    = pathDown(5)
 conPthDwn  =  concatenatedPathDown(6)   admDwn    = administrativelyDown(7)
 rctPthDwn  =  reverseConcatenatedPathDown(8)

 Local       Neighbor               Tx         Rx       Echo Tx   Last Down   Up
 Discr       Address              Packets    Packets    Packets   Diag Code  Count
------+------------------------+----------+----------+----------+---------+-------
 1     100.1.1.10                0          0          5772       0         1
 2     101.1.1.11                5242       5241       0          0         1

-> show ip bfd sessions statistics 1
Tx packet counter                = 0,
Rx packet counter                = 0,
Tx Echo packet counter           = 5772,
Rx Echo packet counter           = 5774,
Session Up Time                  = 6160400,
Session Down Time                = 0,
Last Down Diagnostic Code        = 0,
Session Up Count                 = 1

-> show ipv6 bfd sessions statistics
Legends:
 noDiag     =  noDiagnostic(0)           ctlDetExp = controlDetectionTimeExpired(1)
 echFail    =  echoFunctionFailed(2)     nbrDwn    = neighborSignaledSessionDown(3)
 fwdPlRst   =  forwardingPlaneReset(4)   pthDwn    = pathDown(5)
 conPthDwn  =  concatenatedPathDown(6)   admDwn    = administrativelyDown(7)
 rctPthDwn  =  reverseConcatenatedPathDown(8)
```

```
 Local       Neighbor                Tx         Rx       Echo Tx   Last Down   Up
 Discr       Address               Packets    Packets    Packets   Diag Code  Count
------+-----------------------+----------+----------+----------+---------+-------
 1     fe80::2efa:a2ff:fe13:e402  0          0          5772       0         1

-> show ipv6 bfd sessions statistics 1
Tx packet counter                = 0,
Rx packet counter                = 0,
Tx Echo packet counter           = 5772,
Rx Echo packet counter           = 5774,
Session Up Time                  = 6160400,
Session Down Time                = 0,
Last Down Diagnostic Code        = 0,
Session Up Count                 = 1
```

output definitions

Local Discr	The local discriminator.
Neighbor address	The IP address of the BFD neighbor.
Tx Packets	Number of BFD Control packets transmitted on this session.
Rx Packets	Number of BFD Control packets received on this session.
Echo Tx Packets	Number of BFD Echo packets transmitted on this session.
Last Down Diag Code	Diagnostic code for last session down event.
Up Count	Number of times the session has moved to an UP state since the system was last reset or initialized.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip bfd admin-state	Configures BFD at global level.
ip|ipv6 bfd interface	Configures BFD at interface level.
show ip|ipv6 bfd sessions	Displays the IPv4 or IPv6 BFD sessions for the switch.

MIB Objects

```
alaBfdSessPerfTable
    alaBfdSessPerfPktIn
    alaBfdSessPerfPktOut
    alaBfdSessPerfEchoOut
    alaBfdSessPerfEchoIn
    alaBfdSessPerfUpTime
    alaBfdSessPerfLastSessDownTime
    alaBfdSessPerfLastCommLostDiag
    alaBfdSessPerfSessUpCount
    alaBfdSessPerfDiscTime
```

24 DHCP Relay Commands

Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) packets contain configuration information for network hosts. DHCP Relay enables forwarding of BOOTP/DHCP packets between networks. This allows routing of DHCP traffic between clients and servers. It is not necessary to enable DHCP Relay if DHCP traffic is bridged through one network (the clients and servers are on the same physical network).

This chapter includes a description of DHCP Relay commands that are used to define the IP address of DHCP servers, maximum number of hops, and forward delay time. Configure DHCP Relay on the switch where routing of BOOTP/DHCP packets occur. These CLI commands are applicable for all VRF instances.

MIB information for DHCP Relay commands is as follows:

Filename: ALCATEL-IND1-UDP-RELAY-MIB.mib
Module: alcatelIND1UDPRelayMIB

A summary of the available commands is listed here.

IP DHCP Relay	**ip dhcp relay admin-state** **ip dhcp relay destination** **ip dhcp relay per-interface-mode** **ip dhcp relay interface destination** **ip dhcp relay interface admin-state** **ip dhcp relay forward-delay** **ip dhcp relay maximum-hops** **ip dhcp relay insert-agent-information** **ip dhcp relay insert-agent-information policy** **ip dhcp relay insert-agent-information format** **ip dhcp relay pxe-support** **show ip dhcp relay interface** **show ip dhcp relay statistics** **ip dhcp relay clear statistics** **show ip dhcp relay insert-agent-information error-count** **ip dhcp relay clear insert-agent-information error-count** **show ip dhcp relay counters**
Generic IP UDP Relay	**ip udp relay port** **ip udp relay service** **ip udp relay vlan** **ip udp relay svc** **ip udp relay address** **show ip udp relay** **show ip udp relay statistics** **ipv6 udp relay clear statistics**

Generic IPv6 UDP Relay	**ipv6 udp relay port** **ipv6 udp relay service** **ipv6 udp relay vlan** **ipv6 udp relay svc** **ipv6 udp relay address** **show ipv6 udp relay** **show ipv6 udp relay statistics** **ipv6 udp relay clear statistics**
IPv6 DHCP Relay	**ipv6 dhcp relay admin-state** **ipv6 dhcp relay interface admin-state** **ipv6 dhcp relay destination** **ipv6 dhcp relay maximum-hops** **show ipv6 dhcp relay**
DHCP Server Commands	**dhcp-server** **dhcp-server restart** **show dhcp-server leases** **show dhcp-server statistics** **clear dhcp-server statistics** **dhcpv6-server** **dhcpv6-server restart** **show dhcpv6-server leases** **clear dhcpv6-server statistics** **show dhcpv6-server statistics** **dhcp-message-service** **dhcp-message-service restart** **show message-service status** **active-lease-service** **active-lease-service restart** **show active-lease-service status**

DHCP Snooping	**dhcp-snooping admin-state** **dhcp-snooping mac-address-verification** **dhcp-snooping option-82-data-insertion** **dhcp-snooping bypass option-82-check** **dhcp-snooping option-82 format** **dhcp-snooping option-82 policy** **dhcp-snooping vlan** **dhcp-snooping port** **dhcp-snooping linkagg** **dhcp-snooping ip-source-filter admin-state** **dhcp-snooping ip-source-filter** **dhcp-snooping binding admin-state** **dhcp-snooping binding timeout** **dhcp-snooping binding action** **dhcp-snooping binding persistency** **dhcp-snooping binding** **show dhcp-snooping** **show dhcp-snooping ip-source-filter** **show dhcp-snooping vlan** **show dhcp-snooping port** **dhcp-snooping clear violation-counters** **show dhcp-snooping counters** **dhcp-snooping clear counters** **show dhcp-snooping isf-statistics** **dhcp-snooping clear isf-statistics** **show dhcp-snooping binding**
DHCPv6 Snooping	**dhcpv6-snooping vlan admin-state** **dhcpv6-snooping global admin-state** **dhcpv6-snooping binding timeout** **dhcpv6-snooping binding action** **dhcpv6-snooping binding persistency** **dhcpv6-snooping ipv6-source-filter** **ipv6 dhcp guard** **ipv6 dhcp guard trusted** **show dhcpv6-snooping** **show dhcpv6-snooping interfaces** **show dhcpv6-snooping binding** **show dhcpv6-snooping ipv6-source-filter** **show ipv6 dhcp guard**

ip dhcp relay admin-state

Enables or disables DHCP Relay for the switch for both the VLAN and Shortest Path Bridging (SPB) service domains. When enabled, DHCP packets can be relayed between a client and a server across VLANs or an SPB service domain.

ip dhcp relay admin-state {enable | disable}

Syntax Definitions

enable	Enables DHCP Relay for the VLAN and service domain.
disable	Disables DHCP Relay for the VLAN and service domain.

Defaults

By default, DHCP Relay is disabled for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Disabling this feature does not remove the DHCP relay agent configuration from the switch. However, the configuration is not active unless the feature is enabled using this command.
- When this feature is enabled, DHCP packets are relayed on a global basis or on a per-interface basis.
  - Global DHCP Relay requires a global destination IP address (configured through the **ip dhcp relay destination** command). All DHCP packets are forwarded by a global relay agent.
  - Per-interface DHCP Relay is disabled by default. To enable this mode and define a per-interface relay agent, use the **ip dhcp relay per-interface-mode** and **ip dhcp relay interface destination** commands. Only DHCP packets originating from the VLAN or SPB service that is associated with the specified IP interface are forwarded by the interface relay agent.
  - The global and per-interface modes are mutually exclusive.
  - The global or per-interface mode configuration is not active unless the DHCP Relay feature is enabled for the switch.
- Configure DHCP Relay on switches where packets are routed between IP networks.
- Configuring a DHCP relay agent for an IP interface that is bound to an SPB service (a service-based IP interface) is supported only on the OmniSwitch 9900.

Examples

```
-> ip dhcp relay admin-state enable
-> ip dhcp relay admin-state disable
```

Release History

Release 8.5R3; command introduced.

Related Commands

ip dhcp relay destination	Configures a global destination IP address.
ip dhcp relay per-interface-mode	Enables or disables the per-interface DHCP relay mode, which is used to process DHCP packets on a per-interface basis.
show ip dhcp relay interface	Displays the DHCP Relay configuration.

MIB Objects

```
alaDhcpRelayGlobalConfig
   alaDhcpRelayAdminStatus
```

ip dhcp relay destination

Configures a global destination IP address. When the global DHCP Relay mode is active, all DHCP client requests are forwarded to the specified destination IP address.

ip dhcp relay destination *ip_address*

no ip dhcp relay destination *ip_address*

Syntax Definitions

ip_address	The Pv4 address (for example 21.0.0.10) of the DHCP server to which packets are relayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove the configured DHCP relay destination.
- Configuring a global destination IP address is required when the global DHCP Relay mode is enabled for the switch.

Examples

```
-> ip dhcp relay destination 3.3.0.2
-> ip dhcp relay destination 4.4.0.2
-> no ip dhcp relay destination 3.3.0.2
```

Release History

Release 8.5R3; command introduced.

Related Commands

ip dhcp relay admin-state	Configures the status of the DHCP Relay feature.
show ip dhcp relay interface	Displays the DHCP Relay configuration.

MIB Objects

```
alaDhcpRelayServerDestinationTable
   alaDhcpRelayServerDestinationAddressType,
   alaDhcpRelayServerDestinationAddress,
   alaDhcpRelayServerDestinationRowStatus
```

ip dhcp relay per-interface-mode

Enables or disables the DHCP Relay per-interface mode. When this mode is enabled, a relay agent can be configured for a specific IP interface.

ip dhcp relay per-interface-mode

no ip dhcp relay per-interface-mode

Syntax Definitions

N/A

Defaults

By default, the global DHCP Relay mode is active when the DHCP Relay feature is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the per-interface DHCP relay mode is enabled with this command, the global DHCP relay mode is not available. These two types of relay agents are mutually exclusive.
- Use the **no** form of this command to change the DHCP Relay mode back to global (the default).
- When the per-interface mode is active, use the **ip dhcp relay interface destination** command to configure a destination IP address for each IP interface that will serve as a DHCP relay agent.
- The global or per-interface mode configuration is not active unless the DHCP Relay feature is enabled for the switch.

Examples

```
-> ip dhcp relay per-interface-mode
-> no ip dhcp relay per-interface-mode
```

Release History

Release 8.5R3; command introduced.

Related Commands

ip dhcp relay interface destination	Configures the DHCP relay destination address for the specified IP interface.
ip dhcp relay interface admin-state	Enables or disables the per-interface DHCP relay agent.
ip dhcp relay admin-state	Enables or disables the DHCP relay feature.
show ip dhcp relay interface	Displays the DHCP Relay configuration.

MIB Objects

```
alaDhcpRelayGlobalConfig
   alaDhcpRelayPerInterfaceMode
```

ip dhcp relay interface destination

Configures a DHCP relay destination IP address for the specified interface. The specified IP interface is bound to a VLAN or an SPB service; packets destined for the specified IP address are relayed over the VLAN or SPB service domain.

ip dhcp relay interface *if_name* **destination** *ip_address*

no ip dhcp relay interface *if_name* **destination** *ip_address*

Syntax Definitions

if_name	The name of an IPv4 interface on which a destination IP address is configured. Specify the primary IP interface for the VLAN or service.
ip_address	The Pv4 address (for example 21.0.0.10) of the DHCP server to which packets are relayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the configured DHCP relay destination for the specified interface.
- This command works only if the per-interface DHCP mode is active. Use the **ip dhcp relay per-interface-mode** command to enable this option.
- Configure DHCP Relay on switches where packets are routed between IP networks.
- The IP interface must be defined for a VLAN or an SPB service before using this command. Packets destined for the specified IP address are relayed over the VLAN or SPB service domain.
- Configuring a DHCP relay agent for an IP interface that is bound to an SPB service (a service-based IP interface) is supported only on the OmniSwitch 9900.

Examples

```
-> ip dhcp relay interface client_traffic destination 75.0.0.10
-> ip dhcp relay interface client_traffic destination 31.0.0.20
-> no ip dhcp relay interface client_traffic destination 31.0.0.20
```

Release History

Release 8.5R3; command introduced.

Related Commands

ip dhcp relay per-interface-mode	Enables or disables the DHCP Relay per-interface mode.
ip dhcp relay interface admin-state	Enables or disables DHCP relay on an IP interface.
show ip dhcp relay interface	Displays the DHCP Relay configuration.

MIB Objects

```
dhcpRelayInterfaceTable
   dhcpRelayInterfaceName
   dhcpRelayInterfacIpAddressType
   dhcpRelayInterfacIpAddress
   dhcpRelayInterfacStatus
```

ip dhcp relay interface admin-state

Enables or disables the relay of DHCP packets received on the specified interface.

ip dhcp relay interface *if_name* **admin-state {enable | disable}**

Syntax Definitions

if_name	The name of an IPv4 interface.
enable	Enables the relay of DHCP packets on the interface.
disable	Disables the relay of DHCP packets on the interface.

Defaults

By default, DHCP relay is enabled for the interface when a relay destination IP address is configured for the interface.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

At least one relay destination must be configured before the DHCP relay is enabled for an interface.

Examples

```
-> ip dhcp relay interface client_traffic admin-state enable
-> ip dhcp relay interface client-traffic admin-state disable
```

Release History

Release 8.5R3; command introduced.

Related Commands

ip dhcp relay per-interface-mode	Enables or disables the DHCP Relay per-interface mode.
ip dhcp relay interface destination	Configures the DHCP relay destination address for the specified IP interface.
show ip dhcp relay interface	Displays the DHCP Relay configuration.

MIB Objects

```
alaDhcpRelayInterfaceAdminStateTable
   alaDhcpRelayInterfaceAdminStatus
```

ip dhcp relay forward-delay

Sets the forward delay time value for the DHCP Relay configuration. The BOOTP/DHCP packet sent from the client contains the elapsed boot time. This is the amount of time, in seconds, since the client last booted. DHCP Relay does not process the packet unless the elapsed boot time value of the client is equal to or greater than the configured value of the forward delay time.

ip dhcp relay forward-delay *seconds*

Syntax Definitions

seconds	Forward delay time value in seconds.

Defaults

By default, the forward delay time is set to 0 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The time specified applies to all defined DHCP Relay agent IP addresses.
- If a packet contains an elapsed boot time value that is less than the specified forward delay time value, DHCP Relay discards the packet.

Examples

```
-> ip dhcp relay forward-delay 300
-> ip dhcp relay forward-delay 120
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; **ip helper forward-delay** changed to **ip dhcp relay forward-delay**.

Related Commands

ip dhcp relay admin-state	Enables or disables the DHCP Relay feature for the switch.
ip dhcp relay maximum-hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip dhcp relay interface	Displays current DHCP Relay configuration information.
show ip dhcp relay statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
alaDhcpRelayGlobalConfig
   alaDhcpRelayForwardDelay
```

ip dhcp relay maximum-hops

Sets the maximum number of hops value for the DHCP Relay configuration. This value specifies the maximum number of relays a BOOTP/DHCP packet is allowed to traverse until it reaches its server destination. Limiting the number of hops that can forward a packet prevents packets from looping through the network.

ip dhcp relay maximum-hops *hops*

Syntax Definitions

hops	The maximum number of relays.

Defaults

By default, the maximum hops value is set to 16 hops.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a packet contains a hop count equal to or greater than the *hops* value, DHCP Relay discards the packet.
- The maximum hops value only applies to DHCP Relay and is ignored by other services.

Examples

```
-> ip dhcp relay maximum-hops 1
-> ip dhcp relay maximum-hops 10
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; **ip helper maximum-hops** changed to **ip dhcp relay maximum-hops**

Related Commands

ip dhcp relay admin-state	Enables or disables the DHCP Relay feature for the switch.
ip dhcp relay forward-delay	Sets the forward delay time value. DHCP Relay does not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
show ip dhcp relay interface	Displays current DHCP Relay configuration information.
show ip dhcp relay statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
alaDhcpRelayGlobalConfig
   alaDhcpRelayMaximumHops
```

ip dhcp relay insert-agent-information

Enables or disables the DHCP relay agent information option (Option-82) feature. When this feature is enabled, local relay agent information is inserted into client DHCP packets when the agent forwards these packets to a DHCP server.

ip dhcp relay insert-agent-information

no ip dhcp relay insert-agent-information

Syntax Definitions

N/A

Defaults

By default, this feature is disabled on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the DHCP Option-82 feature.
- This command enables the DHCP Option-82 feature for the entire switch; it is not configurable on a per-interface basis.
- When the relay agent receives a DHCP packet that already contains the Option-82 field, the packet is processed based on the agent information policy configured for the switch. This policy is configured using the **ip dhcp relay insert-agent-information policy** command.
- The DHCP Relay agent information option and DHCP Snooping are mutually exclusive. If the DHCP Relay Option-82 feature is enabled for the switch, then DHCP Snooping is not available. The reverse is also true; if DHCP Snooping is enabled, then DHCP Relay Option-82 is not available

Examples

```
-> ip dhcp relay insert-agent-information
-> no ip dhcp relay insert-agent-information
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; **ip helper agent-information** changed to **ip dhcp relay insert-agent-information**.

Related Commands

ip dhcp relay insert-agent-information policy	Configures a policy to determine how the relay agent handles DHCP packets that already contain the Option-82 field.
ip dhcp relay insert-agent-information format	Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.
show ip dhcp relay interface	Displays current DHCP Relay configuration information.
show ip dhcp relay statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
alaDhcpRelayGlobalConfig
   alaDhcpRelayInsertAgentInformation
```

ip dhcp relay insert-agent-information policy

Configures a policy that determines how the DHCP relay agent handles the DHCP packets that already contain an Option-82 field.

ip dhcp relay insert-agent-information policy {drop | keep | replace}

Syntax Definitions

drop	Drop DHCP packets that already contain an Option-82 field.
keep	Keep the existing Option-82 field information and continue to relay the DHCP packet.
replace	Replace the existing Option-82 field information with local relay agent information and continue to relay the DHCP packet.

Defaults

By default, DHCP packets that already contain an Option-82 field are dropped.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The agent information policy is not applied if the DHCP relay agent receives a DHCP packet from a client that contains a non-zero value for the gateway IP address (giaddr). In this case, the agent does not insert the relay agent information option into the DHCP packet and forwards the packet to the DHCP server.
- Note that if a DHCP packet contains a gateway IP address (giaddr) value that matches a local subnet and also contains the Option-82 field, the packet is dropped by the relay agent.

Examples

```
-> ip dhcp relay insert-agent-information policy drop
-> ip dhcp relay insert-agent-information policy keep
-> ip dhcp relay insert-agent-information policy replace
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; **ip helper agent-information policy** changed to **ip dhcp relay insert-agent-information policy**.

Related Commands

ip dhcp relay insert-agent-information	Enables the insertion of relay agent information Option-82 into DHCP packets.
show ip dhcp relay interface	Displays current DHCP Relay configuration information.
show ip dhcp relay statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
alaDhcpRelayGlobalConfig
   alaDhcpRelayInsertAgentInformationPolicy
```

ip dhcp relay insert-agent-information format

Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.

ip dhcp relay insert-agent-information format {base-mac | system-name | user-string *string* | **interface-alias | auto-interface-alias | ascii {{circuit-id | remoted-id} {base-mac | cvlan | interface | interface-alias | system-name | user-string** *string* | **vlan}} {delimiter** *string***}]}**

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The system name of the switch.
string	A user defined text string. Supports up to 64 characters.
interface-alias	The alias configured for the interface.
auto-interface-alias	The switch automatically generates the interface-alias in the following format: *SystemName_slot_port*.
ascii	ASCII format. **base-mac**: The base MAC address of the switch. **cvlan**: The Customer VLAN ID. **interface**: The interface name. **interface-alias**: The alias configured for the interface. **system-name**: The system name of the switch. **user-string**: A user defined text string. **vlan**: The VLAN ID of which the client is a member. string: A user-defined text string. **delimiter**: The delimiter character that separates fields within the Circuit ID and Remote ID ASCII string value. Valid characters are | (pipe), \ (backward slash), / (forward slash), - (dash), _ (underscore), and " " (space).

Defaults

parameter	default
base-mac | system-name | user-string *string* **| interface-alias | auto-interface-alias | ascii**	**base-mac**
ascii	**base-mac**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The string parameter specifies user-defined information to insert into the Circuit ID and Remote ID fields.
- When entering a *string* for user-defined Option-82 information, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the *string* “Building B Server” requires quotes because of the spaces between the words.
- The **interface-alias** parameter will use the alias configured with the **interfaces alias** command. If no alias is configured a NULL string will be inserted.
- A maximum of 63 characters can be inserted when using the **interface-alias** and **auto-interface-alias** parameters, remaining characters will be truncated.
- The Option-82 format option is a global setting, the format specified is applied to all ports on the switch.
- The data specified with this command is added to the Circuit ID and Remote ID fields only when DHCP Option-82 data insertion is enabled for the switch.
- The ASCII option is used to specify the type of information that is configured in ASCII text string format and then inserted into the Option-82 Circuit ID suboption. Each parameter provided with this command represents a different type of information.
  - Configuring the Circuit ID or Remote ID suboption in ASCII format allows up to five fields (types) of information within the ASCII string. However, if the contents of all the fields combined exceeds 127 characters, then the ASCII string is truncated.
  - Specifying at least one parameter with ASCII option is required. If multiple parameters are selected, then specifying one of the valid delimiter characters is also required.
  - To ensure that the “\” (backward slash) delimiter is parsed correctly, enter two backward slashes in quotes (for example, “\\”).

Examples

```
-> ip dhcp relay insert-agent-information format user-string “Building B Server”
-> ip dhcp relay insert-agent-information format system-name
-> ip dhcp relay insert-agent-information format base-mac
-> ip dhcp relay insert-agent-information format interface-alias
-> ip dhcp relay insert-agent-information format auto-interface-alias
-> ip dhcp relay insert-agent-information format ascii circuit-id user-string “Bldg
A Server”
-> ip dhcp relay insert-agent-information format ascii remote-id vlan system-name
delimiter |
-> ip dhcp relay insert-agent-information ascii interface system-name delimiter
“\\”
```

Release History

Release 8.1.1; command introduced.
Release 8.6R1; **ip helper option-82 format** changed to **ip dhcp relay insert-agent-information format**, **circuit-id** and **remote-id** parameter options added.

Related Commands

show ip dhcp relay interface	Displays the current DHCP configuration for the switch.

MIB Objects

```
alaDhcpRelayGlobalConfig
   alaDhcpRelayOption82FormatType
alaDhcpRelayOption82FormatASCIIConfTable
   alaDhcpRelayOption82FormatASCIIConfField1
   alaDhcpRelayOption82FormatASCIIConfField2
   alaDhcpRelayOption82FormatASCIIConfField3
   alaDhcpRelayOption82FormatASCIIConfField4
   alaDhcpRelayOption82FormatASCIIConfField5
   alaDhcpRelayOption82FormatASCIIConfDelimiter
   alaDhcpRelayOption82FormatASCIIConfStatus
```

ip dhcp relay pxe-support

Enables or disables relay agent support for Preboot Execution Environment (PXE) devices.

ip dhcp relay pxe-support

no dhcp relay pxe-support

Syntax Definitions

N/A

Defaults

By default, PXE support is disabled for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to disable PXE support.

Examples

```
-> ip dhcp relay pxe-support
-> no ip dhcp relay pxe-support
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; **ip helper pxe-support** changed to **ip dhcp relay pxe-support**.

Related Commands

show ip dhcp relay interface	Displays current DHCP Relay configuration information.

MIB Objects

```
alaDhcpRelayGlobalConfig
  alaDhcpRelayPxeSupport
```

show ip dhcp relay interface

Display the DHCP Relay and Relay Agent information.

show ip dhcp relay interface

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- DHCP packets are relayed on a global basis or on a per-interface basis.
- When the global DHCP Relay mode is active (the default), a global destination IP address is required. Global destination IP addresses are displayed in the **Relay Destination list** field.
- When the per-interface DHCP Relay mode is enabled, destination IP addresses are configured for specific interfaces. The **Relay Destination list** displays these IP addresses along with the name of the IP interface associated with each address.

Examples

```
-> show ip dhcp relay interface
IP DHCP Relay :
  DHCP Relay Admin Status        = Disable,
  Forward Delay(seconds)         = 0,
  Max number of hops             = 16,
  Relay Agent Information        = Disabled,
  Relay Agent Information Policy = Drop,
  DHCP Relay Opt82 Format        = Base MAC,
  DHCP Relay Opt82 String        = 00:e0:b1:e7:09:a3,
  PXE support                    = Disabled,
  Relay Mode                     = Global,
  Bootup Option                  = Disable,
  Relay Destination list (Global Mode):
    From Interface Any to Server 128.100.16.1

-> show ip dhcp relay interface
IP DHCP Relay :
  DHCP Relay Admin Status        = Enable,
  Forward Delay(seconds)         = 0,
  Max number of hops             = 16,
  Relay Agent Information        = Disabled,
  Relay Agent Information Policy = Drop,
  DHCP Relay Opt82 Format        = Base MAC,
  DHCP Relay Opt82 String        = 2c:fa:a2:13:e4:02,
```

```
PXE support                    = Disabled,
Relay Mode                     = Per Interface,
Bootup Option                  = Disable,
Relay Destination list (Per Interface Mode):
  From Interface ipvpn1 to Server 50.3.3.1
```

output definitions

DHCP Relay Admin Status	The status (**Enable** or **Disable**) of DHCP Relay. Configured through the **ip dhcp relay admin-state** command.
Forward Delay (seconds)	The current forward delay time. Use the **ip dhcp relay forward-delay** command to change this value.
Max number of hops	The current maximum number of hops allowed. Use the **ip dhcp relay maximum-hops** command to change this value.
Relay Agent Information	Indicates whether the DHCP relay agent information option (Option-82) is **Enabled** or **Disabled**. Configured through the **ip dhcp relay insert-agent-information** command.
Relay Agent Information Policy	The policy configured to determine how the DHCP relay agent handles the DHCP packets that already contain an Option-82 field. Configured through the **ip dhcp relay insert-agent-information policy** command.
DHCP Relay Opt82 Format	The type of Option-82 information inserted. Configured through the **ip dhcp relay insert-agent-information format** command.
DHCP Relay Opt82 String	The Option-82 string based on the specified Option-82 format.
PXE support	Specifies the status (**Enabled** or **Disabled**) of the relay agent support for PXE devices. By default the PXE support is disabled. Configured through the **ip dhcp relay pxe-support** command.
Relay Mode	Whether DHCP Relay is set to operate in the global mode or the per-interface mode. Configured through the **ip dhcp relay per-interface-mode** command.
Bootup Option	Indicates whether or not automatic IP address configuration for a specific VLAN is done when the switch boots up (**Enabled** or **Disabled**). Configured through the **ip interface dhcp-client** command.
Relay Destination list	IP addresses for DHCP servers that receive BOOTP/DHCP packets forwarded by this DHCP Relay service. Use the **ip dhcp relay destination** command (global mode) or **ip dhcp relay interface destination** (per-interface mode) to add or remove DHCP server IP addresses from the DHCP Relay configuration.

Release History

Release 8.5R3; command introduced.
Release 8.6R1; “Relay Agent Information” field added.

Related Commands

show ip dhcp relay statistics	Displays the collected DHCP Relay statistics.

MIB Objects

N/A

show ip dhcp relay statistics

Displays all DHCP Relay statistics collected.

show ip dhcp relay statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The following DHCP Relay statistics are collected:
  - The number of packets DHCP Relay has received.
  - The number of packets dropped due to forward delay, maximum hops, relay agent, and gateway IP violations.
  - Statistics that apply to a specific DHCP server (such as the number of packets transmitted to the server and the number of invalid Option-82 DHCP server packets dropped by the relay agent).
  - The number of packets processed since the last time these statistics were displayed.
- Use the **ip dhcp relay clear statistics** command to clear all DHCP Relay statistics.

Examples

```
-> show ip dhcp relay statistics
Global Statistics :
    Reception From Client :
      Total Count =          12, Delta =        12
    Forw Delay Violation :
      Total Count =          3, Delta =          3
    Max Hops Violation :
      Total Count =          0, Delta =          0
    Agent Info Violation :
      Total Count =          0, Delta =          0
    Invalid Gateway IP :
      Total Count =          0, Delta =          0
Server Specific Statistics :
    From Interface ipv4-v200 to Server 75.0.0.1
        Tx Server :
          Total Count =          9, Delta =          9
        InvAgentInfoFromServer:
          Total Count =          0, Delta =          0
```

output definitions

Reception From Client	Number of packets DHCP Relay has received from the DHCP client.
Forw Delay Violation	Number of packets dropped as a result of forward delay violations. A violation occurs if a client packet contains an elapsed boot time value that is less than the configured DHCP Relay forward delay time value.
Max Hops Violation	Number of packets dropped as a result of maximum hop violations. A violation occurs if a packet contains a hop count equal to or greater than the configured DHCP Relay maximum hops value.
Agent Info Violation	Number of packets dropped as a result of a relay agent information (Option-82) violation. A violation occurs if an Option-82 DHCP packet contains a zero gateway IP address (giaddr) and the relay agent information policy is set to **Drop** or a DHCP packet has no Option-82 field and contains a non-zero giaddr.
Invalid Gateway IP	Number of packets dropped as a result of a gateway IP violation. A violation occurs if an Option-82 DHCP packet contains a gateway IP address (giaddr) that matches a local subnet address.
Delta	Total number of packets processed since the last time the DHCP Relay statistics were checked during any user session.
Server	DHCP server IP address that receives BOOTP/DHCP packets forwarded by this DHCP Relay service.
Tx Server	Number of packets DHCP Relay has transmitted to the DHCP server.
InvAgentInfoFromServer	Number of invalid Option-82 DHCP server packets dropped by the relay agent.
Delta	The difference between the number of packets received from the client and the number of packets transmitted to the DHCP server since the last time DHCP Relay statistics were checked during any user session.

Release History

Release 8.5R3; command introduced.

Related Commands

ip dhcp relay admin-state	Enables or disables the DHCP relay feature.
ip dhcp relay clear statistics	Resets the DHCP Relay statistic counters to zero.
show ip dhcp relay insert-agent-information error-count	Displays the Option-82 related error statistics.

MIB Objects

N/A

ip dhcp relay clear statistics

Clears DHCP relay statistics collected.

ip dhcp relay clear statistics [global-only | destination *ip_address* **| interface** *if_name* **destination** *ip_address***]**

Syntax Definitions

global-only	Clears statistics collected for global DHCP Relay.
ip_address	The IPv4 destination address for which statistics are cleared.
if_name	The IPv4 interface name for which statistics are cleared.

Defaults

By default, all DHCP Relay statistics are cleared.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When this command is used, all DHCP Relay statistics are reset to zero.
- Use the **show ip dhcp relay statistics** command to display DHCP Relay statistics.

Examples

```
-> ip dhcp relay clear statistics
-> ip dhcp relay clear statistics global-only
-> ip dhcp relay clear statistics destination 75.0.0.2
-> ip dhcp relay clear statistics interface ipv4-200 destination 75.0.0.2
```

Release History

Release 8.5R3; command introduced.
Release 8.6R1; **clear ip dhcp relay statistics** changed to **ip dhcp relay clear statistics** and **global-only**, **destination**, **interface** parameters added.

Related Commands

ip dhcp relay admin-state	Enables or disables the DHCP Relay feature.
show ip dhcp relay statistics	Displays DHCP Relay statistics.

MIB Objects

```
alaDhcpRelayGlobalConfig
   alaDhcpRelayStatisticsClear
alaDhcpRelayClearStatisticsTable
   alaDhcpRelayClearStatisticsAction
```

show ip dhcp relay insert-agent-information error-count

Displays the Option-82 related error statistics on a per-port and per-interface basis.

show ip dhcp relay insert-agent-informaton error-count [interface *if_name* **| port** *chassis/slot/port* **[interface** *if_name***]]**

Syntax Definitions

if_name	The name of the IPv4 interface for which the Option-82 error count statistics are displayed.
chassis/slot/port	The chassis, slot, and port number of the port for which the Option-82 error count statistics are displayed.

Defaults

By default, all Option-82 error count statistics are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To display the statistics for a specific port, use the **port** *chassis/slot/port* parameter option.
- To display the statistics for a specific IPv4 interface, use the **interface** *if_name* parameter option.
- Use the **ip dhcp relay clear insert-agent-information error-count** command to clear Option-82 error statistics.

Examples

```
-> show ip dhcp relay insert-agent-information error-count port 1/1/3
 Slot/Port | Interface | Agent Info Violation | Invalid Gateway IP
-----------+-----------+----------------------+----------------------
     1/1/3    ipv4-v100                 500                     0
     1/1/3    ipv4-v200                   0                    10
     1/1/3   ipv4-v1100                 500                     0
     1/1/3   ipv4-v3100                 500                     0

-> show ip dhcp relay insert-agent-information error-count interface ipv4-v100
 Slot/Port | Interface | Agent Info Violation | Invalid Gateway IP
-----------+-----------+----------------------+----------------------
     1/1/1    ipv4-v100                   400                     0
     2/1/3    ipv4-v100                   500                     0

-> show ip dhcp relay insert-agent-information error-count port 1/1/3 interface
ipv4-v100
 Slot/Port | Interface | Agent Info Violation | Invalid Gateway IP
-----------+-----------+----------------------+----------------------
     1/1/3    ipv4-v100                 500                     0
```

output definitions

Slot/port	The chassis, slot, and port number for which the error count statistics is displayed.
Interface	The name of the IPv4 interface associated with the port.
Agent Info Violation	Number of packets dropped as a result of a relay agent information (Option-82) violation. A violation occurs if an Option-82 DHCP packet contains a zero gateway IP address (giaddr) and the relay agent information policy is set to **Drop** or a DHCP packet has no Option-82 field and contains a non-zero giaddr.
Invalid Gateway IP	Number of packets dropped as a result of a gateway IP violation. A violation occurs if an Option-82 DHCP packet contains a gateway IP address (giaddr) that matches a local subnet address.

Release History

Release 8.1.1; command introduced.
Release 8.6.R1; **show ip helper option-82 error-count** changed to **show ip dhcp relay insert-agent-information error-count** and **vlan** changed to **interface**.

Related Commands

ip dhcp relay insert-agent-information format	Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.
show ip dhcp relay interface	Displays current DHCP Relay configuration information.

MIB Objects

```
alaDhcpRelayOpt82ErrStatsTable
   alaDhcpRelayOpt82ErrStatsIfIndex
   alaDhcpRelayOpt82ErrStatsIfName
   alaDhcpRelayOpt82ErrStatsAgentInfoViolation
   alaDhcpRelayOpt82ErrStatsInvalidGatewayIPAddr
```

ip dhcp relay clear insert-agent-information error-count

Clears the Option-82 related error statistics on a per-port and per-interface basis.

ip dhcp relay clear insert-agent-informaton error-count [interface *if_name* **| port** *chassis/slot/port*

Syntax Definitions

if_name	The name of the IPv4 interface for which the Option-82 error count statistics are cleared.
chassis/slot/port	The chassis, slot, and port number of the port for which the Option-82 error count statistics are cleared.

Defaults

By default, all Option-82 error count statistics are cleared.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To clear the statistics for a specific IPv4 interface, use the **interface** *if_name* parameter option.
- To clear the statistics for a specific port, use the **port** *chassis/slot/port* parameter option.
- When this command is used, all Option-82 error statistics are reset to zero.
- Use the **show ip dhcp relay insert-agent-information error-count** command to display Option-82 statistics collected.

Examples

```
-> ip dhcp relay clear insert-agent-information error-count
-> ip dhcp relay clear insert-agent-information error-count interface ipv4-v100
-> ip dhcp relay clear insert-agent-information error-count port 1/1/3
```

Release History

Release 8.6R1; command introduced.

Related Commands

ip dhcp relay insert-agent-information format	Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.
show ip helper	Displays current DHCP Relay configuration information.

MIB Objects

```
alaDhcpRelayOpt82ErrStatsTable
   alaDhcpRelayOpt82ErrStatsReset
```

show ip dhcp relay counters

Displays DHCP Relay packet statistics.

show ip dhcp relay counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display statistics for the various types of DHCP packets that were relayed or passed through by the switch.

Examples

```
-> show ip dhcp relay counters
DHCP Packets:
DHCP Discover Packets                          : 0,
DHCP Offer Packets                             : 0,
DHCP Request Packets                           : 0,
DHCP ACK Packets                               : 0,
DHCP NACK Packets                              : 0,
DHCP Release Packets                           : 0,
DHCP Decline Packets                           : 0,
DHCP Inform Packets                            : 0,
DHCP Renew Packets                             : 0,
```

Release History

Release 8.6R1; command introduced.

Related Commands

ip dhcp relay admin-state	Enables or disables the DHCP relay feature.
show ip dhcp relay statistics	Displays DHCP Relay error statistics.
show ip dhcp relay insert-agent-information error-count	Displays the Option-82 related error statistics.

MIB Objects

N/A

ip helper address

Adds or deletes a DHCP server IP address. DHCP Relay forwards BOOTP/DHCP broadcasts to and from the specified address. If multiple DHCP servers are used, configure one IP address for each server.

ip helper address *ip_address*

no ip helper address [*ip_address***]**

Syntax Definitions

ip_address	DHCP server IP address (for example 21.0.0.10).

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Use the **no** form of this command to delete an IP address from the DHCP Relay service. If an address is not specified, then all addresses are deleted.
- Using this command enables a Global DHCP Relay service on the switch. When the DHCP Relay is specified by the DHCP server IP address, the service is called Global DHCP.
- When the DHCP Relay is specified by the VLAN number of the DHCP request, the service is referred to as Per-VLAN DHCP.
- Global DHCP and Per-VLAN DHCP are mutually exclusive. You can only configure one or the other.
- Use this command to configure DHCP Relay on switches where packets are routed between IP networks.

Examples

```
-> ip helper address 75.0.0.10
-> no ip helper address 31.0.0.20
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use **ip dhcp relay destination**).

Related Commands

ip helper vlan address	Specifies or deletes DHCP Relay based on the VLAN of the DHCP request.
ip dhcp relay forward-delay	Sets the forward delay time value. DHCP Relay does not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
ip dhcp relay maximum-hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperForwAddr
```

ip helper vlan address

Configures a DHCP Relay service for the specified VLAN. This command is used when a per-VLAN only relay service is active on the switch. It does not apply when a standard relay service is used.

ip helper vlan *vlan_id***[-***vlan_id2***] address** *ip_address*

no ip helper vlan *vlan_id***[-***vlan_id2***] address** *ip_address*

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN ID number of the DHCP server VLAN. Use a hyphen to specify a range of VLAN IDs (3-5).
ip_address	IP address (for example 21.0.0.10) of the DHCP server VLAN.

Defaults

If no VLAN identification number is entered, VLAN ID 0 is used by default.

Platforms Supported

Not supported in this release.

Usage Guidelines

- Specifying multiple VLAN IDs and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range of VLAN ID entries. (for example, 10-15).
- The **ip helper vlan address** command works only if the **per-vlan-only** forwarding option is active. Use the **ip helper per-vlan-only** command to enable this option.
- Configure DHCP Relay on switches where packets are routed between IP networks.
- The IP interface must be defined for the VLANs before using this command.
- Use the **no** form of this command to delete the DHCP server VLAN from the DHCP Relay.

Examples

```
-> ip helper vlan 3 address 75.0.0.10
-> ip helper vlan 250-255 address 198.206.15.2
-> no ip helper vlan 3 address 75.0.0.1
-> no ip helper vlan 1601 address 198.206.15.20
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use **ip dhcp relay interface destination**).

Related Commands

ip helper per-vlan-only	Sets the DHCP Relay forwarding option to process only DHCP packets received from a specific, identified VLAN.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperVlan
```

ip helper standard

Sets the DHCP Relay forwarding option to standard. All DHCP packets are processed by a global relay service.

ip helper standard

Syntax Definitions

N/A

Defaults

By default, the DHCP Relay forwarding option is set to **standard**.

Platforms Supported

Not supported in this release.

Usage Guidelines

To process DHCP packets on a per VLAN basis or to change the DHCP Relay forwarding option from standard to per VLAN, use the **ip helper per-vlan-only** command.

Examples

```
-> ip helper standard
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use the **no** form of the **ip dhcp relay per-interface-mode**).

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
show ip helper statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwOption
```

ip helper per-vlan-only

Sets the DHCP Relay forwarding option to process only DHCP packets received from a specific, identified VLAN. This option allows each VLAN to have its own relay.

ip helper per-vlan-only

Syntax Definitions

N/A

Defaults

By default, the UDP forwarding option is set to **standard**.

Platforms Supported

Not supported in this release.

Usage Guidelines

- When the forwarding option is set to **per-vlan-only**, the **standard** (global) DHCP relay service is not available. These two types of services are mutually exclusive.
- To process DHCP packets on a per VLAN basis, or to change the DHCP Relay forwarding option from standard to per VLAN, use the **ip helper per-vlan-only** command.
- Using the **per-vlan-only** forwarding option requires you to specify a DHCP server IP address for each VLAN that provides a relay service. The **ip helper vlan address** command performs this function and at the same time enables relay for the specified VLAN.

Examples

```
-> ip helper per-vlan-only
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use **ip dhcp relay per-interface-mode**).

Related Commands

ip helper vlan address	Configures a DHCP Relay service for the specified VLAN.
ip helper standard	Sets DHCP Relay forwarding option to standard. All DHCP packets are processed.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwOption
```

show ip helper

Displays the current DHCP Relay and Relay Agent Information.

show ip helper

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

Displays information for all IP addresses configured.

Examples

```
-> show ip helper
Ip helper :
  Forward Delay(seconds)         = 300,
  Max number of hops             = 5,
  Relay Agent Information        = Enabled,
  Relay Agent Information Policy = Keep,
  DHCP Opt82 Format              = Base MAC,
  DHCP Opt82 String              = 2c:fa:a2:13:e4:02,
  PXE support                    = Enabled,
  Forward option                 = standard mode,
  Bootup Option                  = Disable,
  Bootup Packet Option           = DHCP
        Forwarding address list (Standard mode):
          128.100.16.1
```

output definitions

Forward Delay	The current forward delay time (default is three seconds). Use the **ip dhcp relay forward-delay** command to change this value.
Max number of hops	The current maximum number of hops allowed (default is four hops). Use the **ip dhcp relay maximum-hops** command to change this value.
Relay Agent Information	Indicates the status (**Enabled** or **Disabled**) of the DHCP relay agent information option feature. Configured through the **ip dhcp relay insert-agent-information** command.
Relay Agent Information Policy	The policy configured to determine how the DHCP relay agent handles the DHCP packets that already contain an Option-82 field. Configured through the **ip dhcp relay insert-agent-information policy** command.

output definitions

DHCP Opt82 Format	The type of option-82 information inserted. Configured through the **ip dhcp relay insert-agent-information format** command.
DHCP Opt82 String	The option-82 string based on the specified Option-82 format.
PXE support	Specifies the status (**Enabled** or **Disabled**) of the relay agent support for PXE devices. By default the PXE support is disabled. Configured through the **ip dhcp relay pxe-support** command.
Forward option	The current forwarding option setting: **standard mode**.
Bootup Option	Indicates whether or not automatic IP address configuration for default VLAN 1 is done when the switch boots up (**Enabled** or **Disabled**). Configured through the **ip interface dhcp-client** command.
Bootup Packet Option	Indicates if the Bootup Option broadcasts a **DHCP** or **BOOTP** packet to obtain an IP address for default VLAN 1.
Forwarding Addresses	IP addresses for DHCP servers that receive BOOTP/DHCP packets forwarded by this DHCP Relay service. Use the **ip helper address** command to add or remove DHCP server IP addresses from the DHCP Relay configuration.

Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use **show ip dhcp relay interface**)

Related Commands

show ip dhcp relay statistics	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperForwAddr
   iphelperForwDelay
   iphelperMaxHops
iphelperAgentInformation
iphelperAgentInformationPolicy
iphelperStatTable
   iphelperBootupOption
   iphelperBootupPacketOption
```

show ip helper statistics

Displays the number of packets DHCP Relay has received, the number of packets dropped due to forward delay and maximum hops violations. It also displays the number of packets processed since the last time these statistics were displayed. It includes statistics that apply to a specific DHCP server, such as the number of packets transmitted to the server and the difference between the number of packets received from a client and the number transmitted to the server.

show ip helper statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

Use the **no ip helper statistics** command to clear DHCP Relay statistics.

Examples

```
-> show ip helper statistics

 Global Statistics :
    Reception From Client :
      Total Count =         12, Delta =         12,
    Forw Delay Violation :
      Total Count =          3, Delta =          3,
    Max Hops Violation :
      Total Count =          0, Delta =          0,
    Agent Info Violation :
      Total Count =          0, Delta =          0,
    Invalid Gateway IP :
      Total Count =          0, Delta =          0,
 Server Specific Statistics :
    From any Vlan to Server 5.5.5.5
        Tx Server :
          Total Count =          9, Delta =          9
        InvAgentInfoFromServer:
          Total Count =          0, Delta =          0
```

output definitions

Reception From Client	Number of packets DHCP Relay has received from the DHCP client.
Forw Delay Violation	Number of packets dropped as a result of forward delay violations. A violation occurs if a client packet contains an elapsed boot time value that is less than the configured DHCP Relay forward delay time value.

output definitions (continued)

Max Hops Violation	Number of packets dropped as a result of maximum hop violations. A violation occurs if a packet contains a hop count equal to or greater than the configured DHCP Relay maximum hops value.
Agent Info Violation	Number of packets dropped as a result of a relay agent information (Option-82) violation. A violation occurs if an Option-82 DHCP packet contains a zero gateway IP address (giaddr) and the relay agent information policy is set to **Drop** or a DHCP packet has no Option-82 field and contains a non-zero giaddr.
Invalid Gateway IP	Number of packets dropped as a result of a gateway IP violation. A violation occurs if an Option-82 DHCP packet contains a gateway IP address (giaddr) that matches a local subnet address.
Server	DHCP server IP address that receives BOOTP/DHCP packets forwarded by this DHCP Relay service. Use the **ip helper address** command to add or remove DHCP server IP addresses from DHCP Relay configuration.
Tx Server	Number of packets DHCP Relay has transmitted to the DHCP server.
Delta	The difference between the number of packets received from the client and the number of packets transmitted to the DHCP server since the last time DHCP Relay statistics were checked during any user session.
Invalid Agent Info From Server	Number of invalid Option-82 DHCP server packets dropped by the relay agent.
Delta	Total number of packets processed since the last time the **ip helper statistics** were checked during any user session.

Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use **show ip dhcp relay statistics**)

Related Commands

show ip dhcp relay interface	Displays current DHCP Relay configuration information.
no ip helper statistics	Resets IP helper statistics.

MIB Objects

```
iphelperStatTable
   iphelperServerAddress
   iphelperRxFromClient
   iphelperTxToServer
   iphelperMaxHopsViolation
   iphelperForwDelayViolation
   iphelperResetAll
```

no ip helper statistics

Resets the IP helper statistics for the specified VRF instances.

no ip helper statistics [global-only | server-only | address *ip_address* | **vlan** *vlan_id* **{address** *ip_address***}]**

Syntax Definitions

global-only	Specifies that only the global IP helper statistics must be reset.
server-only	Specifies that only the IP helper statistics related to the server must be reset.
ip_address	Specifies the IP address for the flat mode instance.
vlan_id	Specifies the VLAN ID for the per-VLAN mode instance.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command works only for VRF instances.
- To reset all the IP helper related statistics, use this command without the additional keywords.
- To reset the IP helper statistics for the flat mode instance, provide the related IP address with the **address** keyword
- To reset the IP helper statistics for the per-vlan mode instance, provide the VLAN ID with the **vlan** keyword and the related IP address with the **address** keyword.

Examples

```
-> no ip helper statistics
-> no ip helper statistics global-only
-> no ip helper statistics server-only
-> no ip helper statistics address 172.6.5.1
-> no ip helper statistics vlan 20 address 172.6.5.1
```

Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use **ip dhcp relay clear statistics**)

Related Commands

show ip helper statistics	Displays the current statistics for each UDP port relay service.

MIB Objects

```
iphelperStatsTable
   iphelperResetAllStats
   iphelperResetSrvStats
```

ip udp relay port

Enables or disables generic UDP relay for the specified UDP service port. A user-defined or well-known UDP port number is specified with this command.

ip udp relay port *port_num* **[description** *description***]**

ip udp relay no port *port_num*

Syntax Definitions

port_num	A UDP service port number (for example, 53, 69, 301).
description	An optional description for the specified UDP service port.

Defaults

By default, relay is enabled on the BOOTP/DHCP well-known ports.

parameter	default
description	UDP port #

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable generic UDP relay for the specified port.
- Use the **ip dhcp relay** commands to configure functionality for BOOTP/DHCP well-known ports (67/68).

Examples

```
-> ip udp relay port 54
-> ip udp relay port 54 description “Generic UDP Service”
-> ip udp relay no port 54

-> ip udp relay port 69 description “TFTP relay”
-> ip udp relay no port 69
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip udp relay vlan	Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.
ip udp relay svc	Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP service port is forwarded
ip udp relay address	Specifies the UDP server IP address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ip udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
genericUdpServiceTable
   genericUdpServiceUdpPort
   genericUdpServiceDescription
   genericUdpServiceRowStatus
```

ip udp relay service

Enables or disables generic UDP relay for the specified UDP service name (NBNS, NBDD, or other well-known UDP ports).

ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} [description *description***]**

ip udp relay no service {tftp | tacacs | ntp | nbns | nbdd | dns}

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
nbns	NBNS well-known ports 137.
nbdd	NBDD well-known port 138.
dns	DNS well-known port 53.
description	An optional description for the specified UDP well-known service port.

Defaults

parameter	default
description	service name and port #

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable UDP Relay for the specified service port.
- The *description* parameter is used with any of the **service** keywords and provides a user-defined description to identify the port service.
- If port relay is enabled for the NBDD well-known port, NBNS is not automatically enabled by default.
- Note that when UDP port relay is enabled for NTP, relay cannot forward NTP packets that contain a destination IP address that matches a VLAN router IP address on the switch.

Examples

```
-> ip udp relay service dns
-> ip udp relay service dns description dns_1
-> ip udp relay no service dns
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip udp relay vlan	Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.
ip udp relay svc	Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP service port is forwarded
ip udp relay address	Specifies the UDP server IP address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ip udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
genericUdpServiceTable
   genericUdpServiceUdpPort
   genericUdpServiceDescription
   genericUdpServiceRowStatus
```

ip udp relay vlan

Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.

ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num* **[description** *description***]} vlan** *vlan_id***[-***vlan_id2***]**

ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num***} no vlan** *vlan_id***[-***vlan_id2***]}**

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
nbns	NBNS well-known ports 137.
nbdd	NBDD well-known port 138.
dns	DNS well-known port 53.
port_num	A user-defined port number.
description	A description of the UDP service.
*vlan_id***[-***vlan_id2***]**	VLAN ID number. Use a hyphen to specify a range of VLAN IDs (3-5).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the VLAN association with the UDP service port.
- The UDP port must be created before using this command.
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.

Examples

```
-> ip udp relay service DNS vlan 10
-> ip udp relay service DNS vlan 500-550
-> ip udp relay service DNS no vlan 10
-> ip udp relay port 3047 vlan 20
-> ip udp relay port 3047 no vlan 20
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip udp relay port	Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
ip udp relay service	Enables or disables generic UDP relay for well-known UDP service names.
ip udp relay svc	Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP port is forwarded
ip udp relay address	Specifies the UDP server IP address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ip udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
genericUdpServiceDstTable
   genericUdpServicePort
   genericUdpServiceDstVlan
   genericUdpServiceDstTblRowStatus
```

ip udp relay svc

Specifies a Shortest Path Bridging (SPB) service on which traffic destined for a UDP port is forwarded.

ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num* **[description** *description***]} svc** *service_id***[-***service_id2***]**

ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num***} no svc** *service_id***[-***service_id2***]**

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
nbns	NBNS well-known ports 137.
nbdd	NBDD well-known port 138.
dns	DNS well-known port 53.
port_num	A user-defined port number.
description	A description of the UDP service.
*service_id***[-***service_id2***]**	SPB service ID number. Use a hyphen to specify a range of service IDs (3-5).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the SPB service association with the UDP service port.
- The UDP port must be created before using this command.
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.

Examples

```
-> ip udp relay service dns svc 10
-> ip udp relay service dns svc 50-55
-> ip udp relay service dns no svc 10
-> ip udp relay port 3047 svc 20
-> ip udp relay port 3047 no svc 20
```

Release History

Release 8.5R4; command introduced.

Related Commands

ip udp relay port	Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
ip udp relay service	Enables or disables generic UDP relay for well-known UDP service names.
ip udp relay vlan	Specifies the VLAN on which traffic destined for the specified UDP port is forwarded.
ip udp relay address	Specifies the UDP server IP address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ip udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
alaGenericUdpServiceSvcTable
    alaGenericUdpServiceSvcPort
    alaGenericUdpServiceDstSvc
    alaGenericUdpServiceSvcRowStatus
```

ip udp relay address

Specifies the UDP server IP address to which traffic destined for a UDP port is forwarded as unicast packets.

ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num* **[description** *description***]} address** *ip_address*

ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num***} no address** *ip_address*

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
nbns	NBNS well-known ports 137.
nbdd	NBDD well-known port 138.
dns	DNS well-known port 53.
port_num	A user-defined port number.
description	A description of the UDP service.
ip_address	The IPv4 address of a UDP server.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the IP address association with the UDP service port.
- The UDP port must be created before using this command.
- Only one IP address can be configured for a UDP port (multiple IP addresses for the same UDP port is not supported).
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.
- When the specified UDP port is associated with an IP address, the relay is operating at the Layer 3 level; any attempt to then assign a VLAN or SPB service to that UDP port is blocked. UDP ports associated with a VLAN or SPB service are operating at the Layer 2 level.

Examples

```
-> ip udp relay service dns address 10.2.2.1
-> ip udp relay service tftp address 20.2.2.1
-> ip udp relay service dns no address 10.2.2.1
```

```
-> ip udp relay port 3047 address 10.2.2.1
-> ip udp relay port 3047 address 10.2.2.1

-> ip udp relay port 54 address 30.2.2.1
-> ip udp relay port 54 vlan 200
ERROR: UDP port configured in L3 mode

-> ip udp relay port 64 vlan 200
-> ip udp relay port 64 address 40.2.2.1
ERROR: UDP port configured in L2 mode
```

Release History

Release 8.3.1; command introduced.

Related Commands

ip udp relay port	Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
ip udp relay service	Enables or disables generic UDP relay for well-known UDP service names.
ip udp relay vlan	Specifies the VLAN on which traffic destined for the specified UDP port is forwarded.
ip udp relay svc	Specifies the Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP port is forwarded.
show ip udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
alaGenericUdpServiceDstIpTable
   alaGenericUdpServiceDstUdpPort
   alaGenericUdpServiceDstIpType
   alaGenericUdpServiceDstIpAddress
   alaGenericUdpServiceDstIpRowStatus
```

show ip udp relay

Displays the generic UDP relay service configuration.

show ip udp relay [service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num***]**

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
nbns	NBNS well-known ports 137.
nbdd	NBDD well-known port 138.
dns	DNS well-known port 53.
port_num	A user-defined or well-known port number.

Defaults

By default, the configuration for all UDP services is shown.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a UDP service name with the **service** parameter to display information about a specific service.
- Enter a UDP service port number with the **port** parameter to display information about a specific user-defined or well-known port.

Examples

```
-> show ip udp relay
 Service Name         Port   IP Address       Vlans      Services
---------------------+------+----------------+---------+--------------------
DNS port              53     40.2.2.1
UDP port 54           54     20.2.2.1
UDP port 55           55                      200
UDP port 56           56                                 10
TFTP port             69                      200        20

-> show ip udp relay port 54
 Service Name         Port   IP Address       Vlans      Services
---------------------+------+----------------+---------+--------------------
UDP port 54           54     20.2.2.1
-> show ip udp relay service tftp
 Service Name         Port   IP Address       Vlans      Services
---------------------+------+----------------+---------+--------------------
TFTP port             69                      200        20
```

output definitions

Service Name	The active UDP service name.
Port	The UDP service port number.
IP Address	The destination IP address assigned to the UDP service port. Configured through the **ip udp relay address** command.
Vlans	The destination VLANs assigned to the UDP service port. Configured through the **ip udp relay vlan** command.
Services	The destination Shortest Path Bridging (SPB) service assigned to the UDP service port. Configured through the **ip udp relay svc** command.

Release History

Release 7.1.1; command introduced.
Release 8.5R4; **IP Address** and **Services** field added.

Related Commands

show ip udp relay statistics	Displays the current statistics for each UDP port relay service.

MIB Objects

N/A

show ip udp relay statistics

Displays the current statistics for each UDP port relay service. These statistics include the name of the service, the forwarding VLANs, Shortest Path Bridging (SPB) services, or an IP address configured for that service, and the number of packets the service has sent and received.

show ip udp relay statistics [service {tftp | tacacs | ntp | nbns | nbdd | dns}] [port [*port_num***]]**

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
nbns	NBNS well-known ports 137.
nbdd	NBDD well-known port 138.
dns	DNS well-known port 53.
port_num	A user-defined or well-known UDP service port number.

Defaults

By default, the statistics for all UDP services is shown.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a UDP service name with the **service** parameter to display information about a specific service.
- Enter a UDP service port number with the **port** parameter to display information about a specific user-define or well-known port.
- Use the **ip udp relay no statistics** command to reset statistics counters.

Examples

```
-> show ip udp relay statistics
Port   Service        Pkts Recvd      Pkts Sent   Dst Vlan/IP Address    Svc
-----+--------------+--------------+-----------+----------------------+-----------
   53 DNS port               0          0             10.1.1.2
   54 UDP port 54            0          0                              10
   55 UDP port 55            0          0             200
   56 UDP port 56            0          0             200
   56 UDP port 56            0          0                              20
   69 TFTP port              0          0             1
                             0          0             300
                             0          0             200
   69 TFTP port              0          0                              20
  123 NTP port               0          0             20.1.1.2
```

```
-> show ip udp relay statistics service tftp
Port   Service        Pkts Recvd      Pkts Sent   Dst Vlan/IP Address    Svc
-----+-------------+--------------+-----------+----------------------+-----------
   69 TFTP port               0          0             1
                              0          0             300
                              0          0             200
   69 TFTP port               0          0                            20

-> show ip udp relay statistics port 53
Port   Service        Pkts Recvd      Pkts Sent   Dst Vlan/IP Address    Svc
-----+-------------+--------------+-----------+----------------------+-----------
   53 DNS port                0          0             10.1.1.2
```

output definitions

Port	The active UDP port number.
Service	The active UDP service name.
Pkts Recvd	The number of packets received by this service port from a client.
Pkts Sent	The number of packets sent from this service port to the server.
Dst Vlan/Ip Address	The VLAN or IP address assigned to the UDP service port that forwards traffic destined for the port. Configured through the **ip udp relay vlan** or **ip udp relay address** command.
Svc	The SPB service assigned to the UDP service port that forwards traffic destined for the port. Configured through the **ip udp relay svc** command.

Release History

Release 7.1.1; command introduced.
Release 8.5R4; **Dst Vlan/IP Address** and **Svc** fields added.

Related Commands

show ip udp relay	Displays current configuration for UDP services by service name or by service port number.
ipv6 udp relay clear statistics	Resets all the generic UDP Relay service statistics.

MIB Objects

N/A

ip udp relay no statistics

Resets all the generic UDP Relay service statistics.

ip udp relay no statistics

Syntax Definitions

N/A

Defaults

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When this command is applied, the UDP relay statistics are cleared and the **show ip udp relay statistics** command displays no information.

Examples

```
-> ip udp relay no statistics
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip udp relay statistics	Displays the current statistics for each UDP port relay service.

MIB Objects

```
genericUdpServiceTable
   genericUdpServiceStatReset
```

ipv6 udp relay port

Enables or disables generic IPv6 UDP relay for the specified UDP service port. A user-defined or well-known UDP port number is specified with this command.

ipv6 udp relay port *port_num* **[description** *description***]**

ipv6 udp relay no port *port_num*

Syntax Definitions

port_num	A UDP service port number (for example, 53, 69, 301).
description	An optional description for the specified UDP service port.

Defaults

By default, relay is enabled on the BOOTP/DHCP well-known ports.

parameter	default
description	UDP port #

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable generic UDP relay for the specified port.
- Use the **ipv6 dhcp relay** commands to configure functionality for BOOTP/DHCP well-known ports (67/68).

Examples

```
-> ipv6 udp relay port 54
-> ipv6 udp relay port 54 description “Generic UDP Service”
-> ipv6 udp relay no port 54

-> ipv6 udp relay port 69 description “TFTP relay”
-> ipv6 udp relay no port 69
```

Release History

Release 8.6R1; command introduced.

Related Commands

ipv6 udp relay vlan	Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.
ipv6 udp relay svc	Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP service port is forwarded
ipv6 udp relay address	Specifies the UDP server IPv6 address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ipv6 udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
alaGenericUdpv6ServiceTable
   alaGenericUdpv6ServiceUdpPort
   alaGenericUdpv6ServiceDescription
   alaGenericUdpv6ServiceRowStatus
```

ipv6 udp relay service

Enables or disables generic IPv6 UDP relay for the specified UDP service name (DNS, NTP, or other well-known UDP ports).

ipv6 udp relay service {tftp | tacacs | ntp | dns} [description *description***]**

ipv6 udp relay no service {tftp | tacacs | ntp | dns}

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
dns	DNS well-known port 53.
description	An optional description for the specified UDP well-known service port.

Defaults

parameter	default
description	service name and port #

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable UDP Relay for the specified service port.
- The *description* parameter is used with any of the **service** keywords and provides a user-defined description to identify the port service.
- Note that when UDP port relay is enabled for NTP, relay cannot forward NTP packets that contain a destination IP address that matches a VLAN router IP address on the switch.

Examples

```
-> ipv6 udp relay service dns
-> ipv6 udp relay service dns description dns_1
-> ipv6 udp relay no service dns
```

Release History

Release 8.6R1; command introduced.

Related Commands

ipv6 udp relay vlan	Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.
ipv6 udp relay svc	Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP service port is forwarded
ipv6 udp relay address	Specifies the UDP server IPv6 address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ipv6 udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
alaGenericUdpv6ServiceTable
   alaGenericUdpv6ServiceUdpPort
   alaGenericUdpv6ServiceDescription
   alaGenericUdpv6ServiceRowStatus
```

ipv6 udp relay vlan

Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.

ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port *port_num* **[description** *description***]} vlan** *vlan_id***[-***vlan_id2***]**

ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port *port_num***} no vlan** *vlan_id***[-***vlan_id2***]}**

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
dns	DNS well-known port 53.
port_num	A user-defined port number.
description	A description of the UDP service.
*vlan_id***[-***vlan_id2***]**	VLAN ID number. Use a hyphen to specify a range of VLAN IDs (for example, 3-5).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the VLAN association with the UDP service port.
- The UDP port must be created before using this command.
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.

Examples

```
-> ipv6 udp relay service dns vlan 10
-> ipv6 udp relay service dns vlan 500-550
-> ipv6 udp relay service dns no vlan 10
-> ipv6 udp relay port 3047 vlan 20
-> ipv6 udp relay port 3047 no vlan 20
```

Release History

Release 8.6R1; command introduced.

Related Commands

ipv6 udp relay port	Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
ipv6 udp relay service	Enables or disables generic UDP relay for well-known UDP service names.
ipv6 udp relay svc	Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP port is forwarded
ipv6 udp relay address	Specifies the UDP server IPv6 address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ipv6 udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
alaGenericUdpv6ServiceDstTable
   alaGenericUdpv6ServiceDstType
   alaGenericUdpv6ServiceDstPort
   alaGenericUdpv6ServiceDstId
   alaGenericUdpv6ServiceDstDescription
   alaGenericUdpv6ServiceDstRowStatus
```

ipv6 udp relay svc

Specifies a Shortest Path Bridging (SPB) service on which traffic destined for a UDP port is forwarded.

ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port *port_num* **[description** *description***]} svc** *service_id***[-***service_id2***]**

ipv6 udp relay service {tftp | tacacs | ntp | dns} | port *port_num***} no svc** *service_id***[-***service_id2***]**

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
dns	DNS well-known port 53.
port_num	A user-defined port number.
description	A description of the UDP service.
*service_id***[-***service_id2***]**	SPB service ID number. Use a hyphen to specify a range of service IDs (3-5).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the SPB service association with the UDP service port.
- The UDP port must be created before using this command.
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.

Examples

```
-> ipv6 udp relay service dns svc 10
-> ipv6 udp relay service dns svc 50-55
-> ipv6 udp relay service dns no svc 10
-> ipv6 udp relay port 3047 svc 20
-> ipv6 udp relay port 3047 no svc 20
```

Release History

Release 8.6R1; command introduced.

Related Commands

ipv6 udp relay port	Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
ipv6 udp relay service	Enables or disables generic UDP relay for well-known UDP service names.
ipv6 udp relay vlan	Specifies the VLAN on which traffic destined for the specified UDP port is forwarded.
ipv6 udp relay address	Specifies the UDP server IPv6 address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ipv6 udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
alaGenericUdpv6ServiceDstTable
   alaGenericUdpv6ServiceDstType
   alaGenericUdpv6ServiceDstPort
   alaGenericUdpv6ServiceDstId
   alaGenericUdpv6ServiceDstDescription
   alaGenericUdpv6ServiceDstRowStatus
```

ipv6 udp relay address

Specifies the UDP server IPv6 address to which traffic destined for a UDP port is forwarded as unicast packets.

ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port *port_num* **[description** *description***]} address** *ipv6_address***]**

ipv6 udp relay service {tftp | tacacs | ntp | dns} | port *port_num* **no address** *ip6_address*

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
dns	DNS well-known port 53.
port_num	A user-defined port number.
description	A description of the UDP service.
ipv6_address	The IPv6 address of a UDP server.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the IPv6 address association with the UDP service port.
- The UDP port must be created before using this command.
- Only one IPv6 address can be configured for a UDP port (multiple IPv6 addresses for the same UDP port is not supported).
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.
- When the specified UDP port is associated with an IPv6 address, the relay is operating at the Layer 3 level; any attempt to then assign a VLAN or SPB service to that UDP port is blocked. UDP ports associated with a VLAN or SPB service are operating at the Layer 2 level.

Examples

```
-> ipv6 udp relay service dns address 2001:DB8:3001::3
-> ipv6 udp relay service tftp address 2001:DB8:3001::3
-> ipv6 udp relay service dns no address 2001:DB8:3001::3
-> ipv6 udp relay port 3047 address 2001:DB8:3001::3
-> ipv6 udp relay port 3047 no address 2001:DB8:3001::3
```

```
-> ipv6 udp relay port 54 address 30.2.2.1
-> ipv6 udp relay port 54 vlan 200
ERROR: UDP port configured in L3 mode

-> ipv6 udp relay port 64 vlan 200
-> ipv6 udp relay port 64 address 40.2.2.1
ERROR: UDP port configured in L2 mode
```

Release History

Release 8.6R1; command introduced.

Related Commands

ipv6 udp relay port	Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
ipv6 udp relay service	Enables or disables generic UDP relay for well-known UDP service names.
ipv6 udp relay vlan	Specifies the VLAN on which traffic destined for the specified UDP port is forwarded.
ipv6 udp relay svc	Specifies the Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP port is forwarded.
show ipv6 udp relay	Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

```
alaGenericUdpv6ServiceDstIpTable
   alaGenericUdpv6ServiceDstUdpPort
   alaGenericUdpv6ServiceDstIpType
   alaGenericUdpv6ServiceDstIpAddress
   alaGenericUdpv6ServiceDstIpRowStatus
```

show ipv6 udp relay

Displays the generic UDP relay service configuration.

show ipv6 udp relay [service {tftp | tacacs | ntp | dns} | port *port_num***]**

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
dns	DNS well-known port 53.
port_num	A user-defined or well-known port number.

Defaults

By default, the configuration for all UDP services is shown.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a UDP service name with the **service** parameter to display information about a specific service.
- Enter a UDP service port number with the **port** parameter to display information about a specific user-defined or well-known port.

Examples

```
-> show ipv6 udp relay
Service Name          Port    IPv6 Address                       Vlans/Services
----------------------+------+----------------------------------+------------------
DNS port              53     3001::3
UDP port 137          137                                       200

-> show ipv6 udp relay port 137
Service Name          Port    IPv6 Address                       Vlans/Services
----------------------+------+----------------------------------+------------------
UDP port 137          137                                       200

-> show ipv6 udp relay service dns
Service Name          Port    IPv6 Address                       Vlans/Services
----------------------+------+----------------------------------+------------------
DNS port              53     3001::3
```

output definitions

Service Name	The active UDP service name.
Port	The UDP service port number.

output definitions (continued)

IPv6 Address	The destination IPv6 address assigned to the UDP service port. Configured through the **ipv6 udp relay address** command.
Vlans	The destination VLANs assigned to the UDP service port. Configured through the **ipv6 udp relay vlan** command.
Services	The destination Shortest Path Bridging (SPB) service assigned to the UDP service port. Configured through the **ipv6 udp relay svc** command.

Release History

Release 8.6R1; command introduced.

Related Commands

show ipv6 udp relay statistics	Displays the current statistics for each UDP port relay service.

MIB Objects

N/A

show ipv6 udp relay statistics

Displays the current statistics for each UDP port relay service. These statistics include the name of the service, the forwarding VLANs, Shortest Path Bridging (SPB) services, or an IPv6 address configured for that service, and the number of packets the service has sent and received.

show ipv6 udp relay statistics [service {tftp | tacacs | ntp | dns}] [port [*port_num***]]**

Syntax Definitions

tftp	TFTP well-known port 69.
tacacs	TACACS well-known port 65.
ntp	NTP well-known port 123.
dns	DNS well-known port 53.
port_num	A user-defined or well-known UDP service port number.

Defaults

By default, the statistics for all UDP services is shown.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a UDP service name with the **service** parameter to display information about a specific service.
- Enter a UDP service port number with the **port** parameter to display information about a specific user-define or well-known port.
- Use the **ipv6 udp relay clear statistics** command to reset statistics counters.

Examples

```
-> show ipv6 udp relay statistics
Port  Service        Pkts Recvd Pkts Sent  Dst Vlan/Svc/IPv6 Address
-----+--------------+----------+----------+----------------------------------------
   53 DNS port                0          0 3001::2
   54 UDP port 54             0          0 10
   55 UDP port 55             0          0 200
   56 UDP port 56             0          0 200
   56 UDP port 56             0          0 20
   69 TFTP port               0          0 1
                              0          0 300
                              0          0 200
   69 TFTP port               0          0 20
  123 NTP port                0          0 2001::2
```

```
-> show ipv6 udp relay statistics service tftp
Port  Service        Pkts Recvd Pkts Sent  Dst Vlan/Svc/IPv6 Address
-----+-------------+----------+----------+---------------------------------------
   69 TFTP port               0          0 1
                              0          0 300
                              0          0 200
   69 TFTP port               0          0 20

-> show ipv6 udp relay statistics port 53
Port  Service        Pkts Recvd Pkts Sent  Dst Vlan/Svc/IPv6 Address
-----+-------------+----------+----------+---------------------------------------
   53 DNS port                0          0 3001::2
```

output definitions

Port	The active UDP port number.
Service	The active UDP service name.
Pkts Recvd	The number of packets received by this service port from a client.
Pkts Sent	The number of packets sent from this service port to the server.
Dst Vlan/Ip Address	The VLAN or IPv6 address assigned to the UDP service port that forwards traffic destined for the port. Configured through the **ipv6 udp relay vlan** or **ipv6 udp relay address** command.
Svc	The SPB service assigned to the UDP service port that forwards traffic destined for the port. Configured through the **ipv6 udp relay svc** command.

Release History

Release 8.6R1; command introduced.

Related Commands

show ipv6 udp relay	Displays current configuration for UDP services by service name or by service port number.
ipv6 udp relay clear statistics	Resets all the generic UDP Relay service statistics.

MIB Objects

N/A

ipv6 udp relay clear statistics

Resets all the generic UDP Relay service statistics.

ipv6 udp relay clear statistics

Syntax Definitions

N/A

Defaults

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When this command is applied, all UDP relay statistics are reset to zero.
- Use the **show ipv6 udp relay statistics** command to display UDP relay statistics.

Examples

```
-> ipv6 udp relay clear statistics
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ipv6 udp relay statistics	Displays the current statistics for each UDP port relay service.

MIB Objects

```
alaGenericUdpv6ServiceGlobal
   alaGenericUdpv6ServiceStatReset
```

ipv6 dhcp relay admin-state

Enables or disables the DHCPv6 Relay feature on a per-VRF basis.

ipv6 dhcp relay admin-state {enable | disable}

Syntax Definitions

enable	Enables the DHCPv6 Relay feature.
disable	Disables the DHCPv6 Relay feature.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

DHCPv6 Relay must be explicitly enabled on the interfaces from which received DHCP client messages are to be relayed.

Examples

```
-> ipv6 dhcp relay admin-state enable
-> ipv6 dhcp relay admin-state disable
```

Release History

Release 7.3.4; command introduced.

Related Commands

ipv6 dhcp relay interface admin-state	Enables or disables the relay of DHCPv6 client messages received on an interface.
show ipv6 dhcp relay	Displays all the interface on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

MIB Objects

```
alaDHCPv6Config
   alaDHCPv6RelayAdminStatus
```

ipv6 dhcp relay interface admin-state

Enables or disables the relay of DHCPv6 client messages received on an interface.

ipv6 dhcp relay *if_name* **admin-state {enable | disable}**

Syntax Definitions

if_name	IPv6 interface name.
enable	Enables the relay of DHCPv6 client messages on an interface.
disable	Disables the relay of DHCPv6 client messages on an interface.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

At least one relay destination must be configured before enabling the DHCPv6 relay on an interface.

Examples

```
-> ipv6 dhcp relay int1 admin-state enable
-> ipv6 dhcp relay int1 admin-state disable
```

Release History

Release 7.3.4; command introduced.

Related Commands

ipv6 dhcp relay destination	Configures the DHCPv6 relay destination.
show ipv6 dhcp relay	Displays all the interface on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

MIB Objects

```
alaDHCPv6RelayInterfaceTable
   alaDHCPv6RelayInterfaceAdminStatus
```

ipv6 dhcp relay destination

Configures the DHCPv6 Relay destination.

ipv6 dhcp relay *if_name* **destination** *ip6_address scope_if_name*

no ipv6 dhcp relay *if_name* **destination** *ip6_address scope_if_name*

Syntax Definitions

if_name	IPv6 interface name.
ip6_address	The IPv6 address of the relay destination.
scope_if_name	Name of the interface for the local-link. This must be specified if the relay destination is a link-local. Not required if the destination address is not a link-local address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Maximum of five relay destinations can be configured for an interface.
- If the relay destination is a link-local address, the name of the interface used to reach the destination must be specified.
- Use the **no** form of the command to remove the configured DHCPv6 Relay destination for an interface.
- The IPv6 interface must be defined for a VLAN or a Shortest Path Bridging (SPB) service before using this command. Packets destined for the specified IPv6 address are relayed over the VLAN or SPB service domain.
- Configuring a DHCPv6 Relay agent for an IPv6 interface that is bound to an SPB service (a service-based IPv6 interface) is supported only on the OmniSwitch 9900.

Examples

```
-> ipv6 dhcp relay int1 destination 2001:DB8:3001::3
-> ipv6 dhcp relay int1 destination fe80::64 int1
-> no ipv6 dhcp relay int1 destination 2001:DB8:3001::3
```

Release History

Release 7.3.4; command introduced.

Related Commands

show ipv6 dhcp relay	Displays all the interface on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

MIB Objects

```
alaDHCPv6RelayDestinationTable
   alaDHCPv6RelayDestinationAddressType
   alaDHCPv6RelayDestinationAddress
   alaDHCPv6RelayDestinationRowStatus
```

ipv6 dhcp relay maximum-hops

Sets the maximum number of hops value for the DHCPv6 Relay configuration. This value specifies the maximum number of relays a DHCPv6 packet is allowed to traverse until it reaches its server destination. Limiting the number of hops that can forward a packet prevents packets from looping through the network.

ip dhcp relay maximum-hops *hops*

Syntax Definitions

hops	The maximum number of relays. The valid range is 1–32.

Defaults

By default, the maximum hops value is set to 32 hops.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a packet contains a hop count equal to or greater than the *hops* value, DHCPv6 Relay discards the packet.
- The maximum hops value only applies to DHCPv6 Relay and is ignored by other services.

Examples

```
-> ipv6 dhcp relay maximum-hops 1
-> ipv6 dhcp relay maximum-hops 10
```

Release History

Release 8.6R1; command introduced.

Related Commands

ipv6 dhcp relay admin-state	Enables or disables the DHCP Relay feature for the switch.
show ipv6 dhcp relay	Displays all the interface on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

MIB Objects

```
alaDHCPv6RelayConfig
   alaDHCPv6RelayMaximumHops
```

show ipv6 dhcp relay

Displays all the interfaces on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

show ipv6 dhcp relay

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Interfaces on which DHCPv6 relay is disabled and which have no relay destinations configured will not be shown in the output.

Examples

```
-> show ipv6 dhcp relay
DHCPv6 Relay: Enabled
Maximum Hops: 32

Interface                  Relay Destination(s)                     Status
---------------------------+----------------------------------------+--------
vlan-41                    ff02::1:2                                Enabled
vlan-103                   2001:dbc8:8003::17                       Disabled
                           2001:dbc8:8004::99
vlan-200                   fe80::cd0:deff:fe28:1ca5 vlan-201        Enabled
tunnel-2                   2001:dbc8:a23::ea77                      Enabled
```

output definitions

DHCPv6 Relay	Specifies if the DHCPv6 Relay feature is enabled in the current VRF.
Maximum Hops	The maximum number of relays the BOOTP/DHCP packet can go through until it reaches its server destination.
Interface	Displays the interface on which DHCPv6 Relay is enabled.
Relay Destination(s)	Displays the configured DHCPv6 Relay destination(s) for the interface.
Status	Displays the status of DHCPv6 Relay on the interface.

Release History

Release 7.3.4; command introduced.
Release 8.6R1; “Maximum Hops” field added.

Related Commands

ipv6 dhcp relay admin-state	Enables or disables the DHCPv6 Relay feature on a per-VRF basis.
ipv6 dhcp relay interface admin-state	Enables or disables the relay of DHCPv6 client messages received on an interface.
ipv6 dhcp relay destination	Configures the DHCPv6 relay destination address.
ipv6 dhcp relay maximum-hops	Configures the maximum number of hops value.

MIB Objects

```
alaDHCPv6RelayConfig
   alaDHCPv6RelayMaximumHops
   alaDHCPv6RelayAdminStatus
alaDHCPv6RelayInterfaceTable
   alaDHCPv6RelayInterfaceEntry
   alaDHCPv6RelayInterfaceAdminStatus
alaDHCPv6RelayDestinationTable
   alaDHCPv6RelayDestinationAddress
```

dhcp-server

Enables or disables the DHCP server operation.

dhcp-server {enable | disable}

Syntax Definitions

enable	Enables the DHCP server.
disable	Disables the DHCP server.

DefaultsDefaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When DHCP server is enabled on the switch, DHCP relay and DHCP snooping will not be supported on the default VRF of the switch.
- DHCP server must be restarted when changes are made to the dhcpd.conf or dhcpd.pcy file. Use the **dhcp-server restart** command to restart the DHCP server.

Examples

```
-> dhcp-server enable
-> dhcp-server disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show dhcp-server leases	Displays the leases offered by the DHCP server.
dhcp-server restart	Allows to restart the DHCP server when the **dhcpd.conf** or **dhcpd.pcy** file is modified.
clear dhcp-server statistics	Clears the statistics of the DHCP server.

MIB Objects

```
alaDhcpSrvGlobalConfigStatus
```

dhcp-server restart

Allows to restart the DHCP server when the dhcpd.conf or dhcpd.pcy file is modified.

dhcp-server restart

Syntax Definitions

restart	Restarts the DHCP server.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The command can be used to restart the DHCP server when the dhcpd.conf or dhcpd.pcy file is modified.

Examples

```
-> dhcp-server restart
```

Release History

Release 7.3.4; command was introduced.

Related Commands

dhcp-server	Enables or disables the DHCP server operation

MIB Objects

```
alaDhcpSrvGlobalRestart
```

show dhcp-server leases

Displays the leases offered by the DHCP server.

show dhcp-server leases [ip- address *ip_address* **| mac-address** *mac_address***] [type {static | dynamic}] [count]**

Syntax Definitions

ip_address	Specifies IP address of the interface configured with DHCP server.
mac_address	Specifies MAC address of the interface configured with DHCP server.
static	Displays only static leases.
dynamic	Displays only dynamic leases.
count	Count of DHCP messages recorded.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

DHCP server should be enabled before using this command.

Examples

```
-> show dhcp-server leases

Total leases: 8

IP Address MAC address        Lease Granted         Lease Expiry          Type
---------+------------------+--------------------+--------------------+-----------
200.0.1.1 00:00:01:b8:91:3f  DEC 15 14:10:59 2009  DEC 19 01:30:59 2009  DYNAMIC
200.0.1.2 00:00:01:b8:91:37  DEC 15 14:11:05 2009  DEC 19 01:31:05 2009  DYNAMIC
200.0.1.3 00:00:01:b8:91:3b  DEC 15 14:11:48 2009  DEC 19 01:31:48 2009  DYNAMIC
200.0.1.4 00:00:01:b8:91:3d  DEC 15 14:11:53 2009  DEC 19 01:31:53 2009  DYNAMIC
220.0.0.2 00:00:01:1d:4f:7e  DEC 15 14:11:45 2009  DEC 15 22:31:45 2009  DYNAMIC
220.0.0.3 00:00:01:5a:0b:76  DEC 15 14:12:00 2009  DEC 15 22:32:00 2009  DYNAMIC
220.0.0.4 00:00:01:1d:4f:7d  DEC 15 14:11:53 2009  DEC 15 22:31:53 2009  DYNAMIC
120.0.0.4 00:00:02:12:4f:8c  DEC 15 14:11:53 2009  DEC 15 23:31:53 2009  STATIC

-> show dhcp-server leases ip-address 200.0.1.2

IP Address MAC address        Lease Granted         Lease Expiry          Type
---------+------------------+--------------------+--------------------+-----------
200.0.1.2 00:00:01:b8:91:37  DEC 15 14:11:05 2009  DEC 19 01:31:05 2009  DYNAMIC
```

```
-> show dhcp-server leases mac-address 00:00:01:1d:4f:7d

IP Address MAC address        Lease Granted         Lease Expiry          Type
----------+-----------------+--------------------+---------------------+----------
220.0.0.4  00:00:01:1d:4f:7d DEC 15 14:11:53 2009 DEC 15 22:31:53 2009  DYNAMIC

-> show dhcp-server leases type static

Total leases: 1

IP Address  MAC address        Lease Granted         Lease Expiry         Type
----------+-----------------+--------------------+--------------------+-----------
120.0.0.4  00:00:02:12:4f:8c DEC 15 14:11:53 2009  DEC 15 23:31:53 2009 STATIC
```

output definitions

IP address	The IP address allocated to the client.
MAC address	The MAC address of the client for which the lease is allocated.
Lease Granted	The date and time at which lease is granted.
Lease Expiry	The date and time at which lease expires.
Type	The type of lease offered.

Release History

Release 7.3.4; command introduced.

Related Commands

clear dhcp-server statistics	Clears the DHCP server lease statistics.

MIB Objects

```
alaDhcpSrvLeaseTable
   alaDhcpSrvLeaseMACAddress
   alaDhcpSrvLeaseIpAddress
   alaDhcpSrvLeaseLeaseGrant
   alaDhcpSrvLeaseLeaseExpiry
   alaDhcpSrvLeaseType
```

show dhcp-server statistics

Displays the statistics of the DHCP server.

show dhcp-server statistics [packets | hosts | subnets | all]

Syntax Definitions

packets	Displays general statistical information along with specific information about data packets received, dropped, and transmitted.
hosts	Displays general statistical information along with specific information about leases related to the DHCP server.
subnets	Displays general statistical information along with specific information about all the subnets.
all	Displays all statistical information related to the DHCP server.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

DHCP server should be enabled before using this command.

Examples

```
-> show dhcp-server statistics
General:
  DHCP Server Name: mample.vitalqip.com,
   DHCP Server Status         : Enabled,
   Total Subnets Managed      : 7,
   Total Subnets Used         : 2,
   Total Subnets Unused       : 5,
   Total Subnets Full         : 0,
   DHCP Server System Up Time : TUE DEC 15 14:10:27.9956
Lease DB Sync time (in sec)  : 60,
       Last sync time        : TUE DEC 15 14:21:34 2009,
       Next sync time        : TUE DEC 15 14:22:34 2009

-> show dhcp-server statistics packets
Packets:
   Total DHCP Discovers       : 12,
   Total DHCP Offers          : 12,
   Total DHCP Requests        : 16,
   Total DHCP Request Grants  : 10,
   Total DHCP Request Renews  : 6,
   Total DHCP Declines        : 0,
   Total DHCP Acks            : 16,
   Total DHCP Nacks           : 0,
```

```
  Total DHCP Releases        : 0,
  Total DHCP Informs         : 0,
  Total Bootp requests       : 0,
  Total Bootp response       : 0,
  Total Unknown packets      : 0

-> show dhcp-server statistics hosts
Leases:
    Total:
      Leases Managed: 1365,
      Leases used              : 7,
      Leases unused            : 1358,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Static DHCP:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Dynamic DHCP:
      Leases Managed           : 1365,
      Leases used              : 7,
      Leases unused            : 1358,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Automatic DHCP:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Static Bootp:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Automatic Bootp           :
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0

-> show dhcp-server statistics subnets
Subnets:
    Subnet1:
      Subnet: 200.0.0.0,
      Total                    : 1022,
      Static DHCP              : 0,
      Dynamic DHCP             : 1022,
      Automatic DHCP           : 0,
      Static Bootp             : 0,
      Automatic Bootp          : 0
        Ranges:
          Start                : 200.0.1.1,
          End                 : 200.0.2.255,
          Mask                : 255.255.253.0,
```

```
            Type                : 5
            Used                : 4,
            Unused              : 507,
            Pending             : 0,
            Unavailable         : 0
        Subnet2:
          Subnet                : 220.0.0.0,
          Total                 : 508,
          Static DHCP           : 0,
          Dynamic DHCP          : 508,
          Automatic DHCP        : 0,
          Static Bootp          : 0,
          Automatic Bootp       : 0
            Ranges:
           Start                : 220.0.0.2,
           End                  : 220.0.0.255,
           Mask                 : 255.255.255.0,
           Type                 : 5,
           Unused               : 251,
           Used                 : 3,
           Pending              : 0,
           Unavailable          : 0
        Subnet3:
          Subnet                : 150.0.0.0,
          Total                 : 400,
          Static DHCP           : 0,
          Dynamic DHCP          : 400,
          Automatic DHCP        : 0,
          Static Bootp          : 0,
          Automatic Bootp       : 0
            Ranges:
              Range1:
                Start           : 150.0.1.1,
                End             : 150.0.1.100,
               Mask             : 255.255.255.0,
                Type            : 5,
                Used            : 0,
                Unused          : 100,
                Pending         : 0,
                Unavailable     : 0
              Range2:
                Start           : 150.0.2.1,
                End             : 150.0.2.100,
                Mask            : 255.255.255.0,
                Type            : 5,
                Unused          : 100,
                Used            : 0,
                Pending         : 0,
                Unavailable     : 0
    Subnet4:
         Subnet                 : 50.0.0.0,
         Total                  : 200,
         Static DHCP            : 0,
         Dynamic DHCP           : 200,
         Automatic DHCP         : 0,
         Static Bootp           : 0,
         Automatic Bootp        : 0
           Ranges:
             Start              : 50.0.1.1,
```

```
           End                : 50.0.1.100,
           Mask               : 255.255.255.0,
          Type               : 5,
           Unused             : 100,
           Used               : 0,
           Pending            : 0,
           Unavailable        : 0

-> show dhcp-server statistics all
General:
  DHCP Server Name: mample.vitalqip.com,
  DHCP Server Status         : Enabled,
  Total Subnets Managed      : 7,
  Total Subnets Used         : 2,
  Total Subnets Unused       : 5,
  Total Subnets Full         : 0,
  DHCP Server System Up Time : TUE DEC 15 14:10:27.9956
    Lease DB Sync:
      DB Sync time (in sec)   : 60,
      Last sync time           : TUE DEC 15 14:21:34 2009,
      Next sync time           : TUE DEC 15 14:22:34 2009
Packets:
  Total DHCP Discovers: 12,
  Total DHCP Offers          : 12,
  Total DHCP Requests        : 16,
  Total DHCP Request Grants  : 10,
  Total DHCP Request Renews  : 6,
  Total DHCP Declines        : 0,
  Total DHCP Acks            : 16,
  Total DHCP Nacks           : 0,
  Total DHCP Releases        : 0,
  Total DHCP Informs         : 0,
  Total Bootp requests       : 0,
  Total Bootp response       : 0,
  Total Unknown packets      : 0
Leases:
    Total:
      Leases Managed: 1365,
      Leases used              : 7,
      Leases unused            : 1358,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Static DHCP:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Dynamic DHCP:
      Leases Managed           : 1365,
      Leases used              : 7,
      Leases unused            : 1358,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Automatic DHCP:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
```

```
        Leases unavailable        : 0
      Static Bootp:
        Leases Managed            : 0,
        Leases used               : 0,
        Leases unused             : 0,
        Leases Pending            : 0,
        Leases unavailable        : 0
      Automatic Bootp            :
        Leases Managed            : 0,
        Leases used               : 0,
        Leases unused             : 0,
        Leases Pending            : 0,
        Leases unavailable        : 0
  Subnets:
      Subnet1:
        Subnet                   : 200.0.0.0,
        Total                     : 1022,
        Static DHCP               : 0,
        Dynamic DHCP              : 1022,
        Automatic DHCP            : 0,
        Static Bootp             : 0,
        Automatic Bootp           : 0
          Ranges:
            Start                : 200.0.1.1,
            End                  : 200.0.2.255,
            Mask                 : 255.255.253.0,
            Type                 : 5
            Used                 : 4,
            Unused               : 507,
            Pending              : 0,
            Unavailable          : 0
      Subnet2:
        Subnet                    : 220.0.0.0,
        Total                     : 508,
        Static DHCP               : 0,
        Dynamic DHCP              : 508,
        Automatic DHCP            : 0,
        Static Bootp              : 0,
        Automatic Bootp           : 0
          Ranges:
            Start                : 220.0.0.2,
            End                  : 220.0.0.255,
            Mask                 : 255.255.255.0,
            Type                 : 5
            Unused               : 251,
            Used                 : 3,
            Pending              : 0,
            Unavailable          : 0
      Subnet3:
        Subnet                    : 150.0.0.0,
        Total                     : 400,
        Static DHCP               : 0,
        Dynamic DHCP              : 400,
        Automatic DHCP            : 0,
        Static Bootp              : 0,
        Automatic Bootp           : 0
          Ranges:
            Range1:
              Start              : 150.0.1.1,
```

```
            End                : 150.0.1.100,
             Mask              : 255.255.255.0,
            Type               : 5,
            Used               : 0,
            Unused             : 100,
            Pending            : 0,
            Unavailable        : 0
          Range2:
            Start              : 150.0.2.1,
            End                : 150.0.2.100,
            Mask               : 255.255.255.0,
            Type               : 5,
            Unused             : 100,
            Used               : 0,
            Pending            : 0,
            Unavailable        : 0
Subnet4:
     Subnet                    : 50.0.0.0,
     Total                     : 200,
     Static DHCP               : 0,
     Dynamic DHCP              : 200,
     Automatic DHCP            : 0,
     Static Bootp              : 0,
     Automatic Bootp           : 0
       Ranges:
         Start                 : 50.0.1.1,
         End                   : 50.0.1.100,
         Mask                  : 255.255.255.0,
          Type                 : 5,
         Unused                : 100,
         Used                  : 0,
         Pending               : 0,
         Unavailable           : 0
```

output definitions

General stats	Denotes general DHCP Server statistics.
Name	Specifies the name assigned to the DHCP server.
Status	Specifies up or down status of the DHCP server.
Total subnets used	Specifies the total number of subnets being used.
Total subnets managed	Specifies the total number of subnets being managed by the DHCP server.
Total subnets unused	Specifies the total number of subnets being unused.
Total subnets full	Specifies the total number of subnets where all the IP addresses are used.
DHCP Server System Up Time	Shows the DHCP Server System Up Time Performance Monitor counter.
Sync time	Specifies the time for DHCP server to contact and synchronize with the designated time server.
Last sync time	Specifies the last time the synchronization occurred.
Next sync time	Specifies the next time the synchronization should be scheduled.
Packet stats	Denotes statistical information about the data packet transmission.

output definitions (continued)

Total DHCP Discovers	Specifies the total number of DHCPDISCOVER packets sent by the clients to the DHCP server.
Total DHCP Offers	Specifies the total number of DHCPOFFER packets sent by the server to the clients.
Total DHCP Requests	Specifies the total number of DHCPREQUEST packets sent by the clients in response to the DHCPOFFER packets.
Total DHCP Request Grants	Specifies the total number of DHCP request grants provided by the server to the clients.
Total DHCP Request Renews	Specifies the total number of DHCP lease renew requests sent by the clients to the DHCP server.
Total DHCP Declines	Specifies the total number of DHCP requests declined by the DHCP server.
Total DHCP Acks	Specifies the total number of DHCPACK acknowledgement packets sent by the DHCP server to the clients.
Total DHCP Nacks	Specifies the total number of DHCP Negative acknowledgements sent from the DHCP server to the clients. The DHCPNACK message is sent when all the IP addresses available to the server are exhausted and the client sends a DHCPREQUEST.
Total DHCP Releases	Specifies the total number of DHCPRELEASE packets sent by the DHCP server to release IP addresses from its clients.
Total DHCP Informs	Specifies the total number of DHCPINFORM packets sent by the clients to obtain DHCP options from the DHCP server.
Total Bootp requests	Specifies the total number of BOOTP requests sent by the clients to the DHCP server.
Total Bootp response	Specifies the total number of BOOTP response packets sent by the DHCP server to the clients.
Total Unknown packets	Specifies the total number of unknown or badly formatted DHCP packets received by the DHCP server.
Leases stats	Denotes statistical information about leases provided by the DHCP server.
Hosts Managed	Specifies the total number of clients managed by the DHCP server.
Hosts used	Specifies the total number of clients using the IP addresses provided by the DHCP server.
Hosts unused	Specifies the total number of clients managed by the DHCP server which are not being used.
Hosts Pending	Specifies the total number of DHCP IP address requests which are pending by the DHCP server.
Hosts unavailable	Specifies the total number of DHCP hosts which are unavailable i.e; whose lease period have expired.
Static DHCP	Denotes statistical information about the hosts configured with Static DHCP.
Automatic DHCP	Denotes statistical information about the hosts configured with Automatic DHCP.

output definitions (continued)

Static BootP	Denotes statistical information about the hosts configured under Static BootP. **Note:** BootP Relay is disabled when DHCP server is enabled on the switch.
Automatic BootP	Denotes statistical information about the hosts configured with Automatic BootP.
Subnet statistics	Denotes all DHCP related statistical information for individual subnets.
Range	Specifies the range of IP addresses in the individual subnet.
Mask	Specifies the subnet mask.
Type	Specifies whether the type of IP address allocation is dynamic or static.

Release History

Release 7.3.4; command introduced.

Related Commands

clear dhcp-server statistics	Clears the DHCP Server lease statistics.

MIB Objects

N/A

clear dhcp-server statistics

Clears the packet counters of DHCP server statistics.

clear dhcp-server statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to clear the packet counters of DHCP server statistics.

Examples

```
-> clear dhcp-server statistics
```

Release History

Release 7.3.4; command introduced.

Related Commands

show dhcp-server statistics	Displays the DHCP Server lease statistics.

MIB Objects

N/A

dhcpv6-server

Enables or disables the DHCPv6 server operation.

dhcpv6-server {enable | disable}

Syntax Definitions

enable	Enables the DHCPv6 server.
disable	Disables the DHCPv6 server.

DefaultsDefaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- The dhcpdv6.conf and dhcpdv6.pcy files will be parsed when the DHCPv6 status is enabled for the first time.
- There will be one instance of DHCPv6 for the default VRF.

Examples

```
-> dhcpv6-server enable
-> dhcpv6-server disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show dhcpv6-server leases	Displays the leases offered by the DHCPv6 server.
dhcpv6-server restart	Allows to restart the DHCPv6 server when the dhcpdv6.conf or dhcpdv6.pcy file is modified.
clear dhcpv6-server statistics	Displays the statistics of the DHCPv6 server.

MIB Objects

```
alaDhcpv6SrvGlobalConfigStatus
```

dhcpv6-server restart

Allows to restart the DHCPv6 server when the dhcpdv6.conf or dhcpdv6.pcy file is modified.

dhcpv6-server restart

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> dhcpv6-server restart
```

Release History

Release 7.3.4; command was introduced.

Related Commands

dhcpv6-server	Enables or disables the DHCPv6 server operation.

MIB Objects

```
alaDhcpv6SrvGlobalRestart
```

show dhcpv6-server leases

Displays the leases offered by the DHCPv6 server.

show dhcpv6-server leases [ip- address *ipv6_address* **| type {static | dynamic}] [count]**

Syntax Definitions

ipv6_address	Specifies IPv6 address of the interface configured with DHCPv6 server.
static	Displays only static leases.
dynamic	Displays only dynamic leases.
count	Count of DHCPv6 messages recorded.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show dhcpv6-server leases

Total leases: 8

IP Address          Lease Granted        Pref Lease Expiry     Valid Lease Expiry   Type
------------------+--------------------+--------------------+-----------
2001:100::2        DEC 15 14:10:59 2009  DEC 19 01:30:59 2009  DEC 19 05:30:59 2009 STATIC
2001:100::3        DEC 15 14:11:05 2009  DEC 19 01:31:05 2009  DEC 19 05:31:05 2009 DYNAMIC
2001:200::2        DEC 15 14:11:48 2009  DEC 19 01:31:48 2009  DEC 19 05:31:48 2009 DYNAMIC

-> show dhcpv6-server leases ip-address 2001:100::3
IP Address          Lease Granted       Pref Lease Expiry      Valid Lease Expiry   Type
------------------+--------------------+--------------------+--------------------+-----
2001:100::3         DEC 15 14:11:05 2009  DEC 19 01:31:05 2009  DEC 19 05:31:05 2009 DYNAMIC

-> show dhcpv6-server leases type static

Total leases: 1
IP Address       Lease Granted       Pref Lease Expiry      Valid Lease Expiry   Type
----------------+------------------+--------------------+--------------------+-------
2001:100::2      DEC 15 14:10:59 2009  DEC 19 01:30:59 2009  DEC 19 05:30:59 2009 STATIC
```

output definitions

IP address	The IP address allocated to the client.
Lease Granted	The date and time at which lease is granted.

output definitions (continued)

Pref Lease Expiry	The date and time at which lease expires.
Type	The type of lease offered.

Release History

Release 7.3.4; command introduced.

Related Commands

clear dhcpv6-server statistics	Clears the DHCPv6 server lease statistics.

MIB Objects

```
alaDhcpv6SrvLeaseTable
   alaDhcpv6SrvLeaseIpAddress
   alaDhcpv6SrvLeaseLeaseGrant
   alaDhcpv6SrvLeaseLeaseExpiry
   alaDhcpv6SrvLeaseType
```

show dhcpv6-server statistics

Displays the statistics of the DHCPv6 server.

show dhcpv6-server statistics [packets | hosts | subnets | all]

Syntax Definitions

packets	Displays general statistical information along with specific information about data packets received, dropped, and transmitted.
hosts	Displays general statistical information along with specific information about leases related to the DHCPv6 server.
subnets	Displays general statistical information along with specific information about all the subnets.
all	Displays all statistical information related to the DHCPv6 server.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

DHCPv6 server should be enabled before using this command.

Examples

```
-> show dhcpv6-server statistics
General:
  DHCPv6 Server Name            : DHCPv6,
  DHCPv6 Server Status          : Enabled,
  Total Subnets Managed         : 4,
  Total Subnets Used            : 0,
  Total Subnets Unused          : 4,
  Total Subnets Full            : 0,
  DHCPv6 Server System Up Time  : Mon Jan 12 05:49:54.198,
    Lease DB Sync time (in sec) : 60,
      Last sync time            : Mon Jan 12 08:41:02 2015,
      Next sync time            : Mon Jan 12 08:42:02 201

-> show dhcpv6-server statistics packets
Packet:
  Total DHCPv6 Solicts              : 0,
  Total DHCPv6 Advertises           : 0,
  Total DHCPv6 Requests             : 0,
  Total DHCPv6 Renews               : 0,
  Total DHCPv6 Rebinds              : 0,
  Total DHCPv6 Declines             : 0,
  Total DHCPv6 Confirms             : 0,
  Total DHCPv6 Replys               : 0,
```

```
  Total DHCPv6 Releases              : 0,
  Total DHCPv6 Information Requests  : 0,
  Total DHCPv6 Lease Querys          : 0,
  Total Delete Leases                : 0,
  Total Unknown packets              : 0

-> show dhcpv6-server statistics leases
Leases:
    Total:
      Leases Managed            : 50190,
      Leases used               : 0,
      Leases unused             : 50190,
      Leases Pending            : 0,
      Leases unavailable        : 0
    Static DHCPv6:
      Leases Managed            : 10,
      Leases used               : 0,
      Leases unused             : 10,
      Leases Pending            : 0,
      Leases unavailable        : 0
    Dynamic DHCPv6:
     Leases Managed            : 50180,
      Leases used               : 0,
      Leases unused             : 50180,
      Leases Pending            : 0,
      Leases unavailable        : 0

-> show dhcpv6-server statistics subnets
Subnets:
  Subnet 1:
    SubnetAddr      : 2620:0:60:1480::,
    Total           : 17666,
    Static DHCP     : 1,
    Dynamic DHCP    : 17665,
        Ranges:
        Range1:
          Start                 : 2620:0:60:1480::1f01,
          End                   : 2620:0:60:1480::1f01,
          PrefixLength          : 97,
          Type                  : 1,
          inUse                 : 0,
          Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
        Range2:
          Start                 : 2620:0:60:1480::2000,
          End                   : 2620:0:60:1480::6500,
          PrefixLength          : 97,
          Type                  : 2,
          inUse                 : 0,
          Unused                : 17665,
          Pending               : 0,
          Unavailable           : 0
Subnet 2:
    SubnetAddr      : 2620:0:60:1481::,
    Total           : 29956,
    Static DHCP     : 3,
    Dynamic DHCP    : 29953,
        Ranges:
```

```
          Range1:
            Start                : 2620:0:60:1481::1f01,
            End                  : 2620:0:60:1481::1f01,
            PrefixLength         : 64,
            Type                 : 1,
            inUse                : 0,
            Unused               : 1,
            Pending              : 0,
            Unavailable          : 0
          Range2:
            Start                : 2620:0:60:1481::1f02,
            End                  : 2620:0:60:1481::1f02,
            PrefixLength         : 64,
            Type                 : 1,
            inUse                : 0,
            Unused               : 1,
            Pending              : 0,
            Unavailable          : 0
         Range3:
            Start                : 2620:0:60:1481::1f03,
            End                  : 2620:0:60:1481::1f03,
            PrefixLength         : 64,
            Type                 : 1,
            inUse                : 0,
            Unused               : 1,
            Pending              : 0,
            Unavailable          : 0
          Range4:
            Start                : 2620:0:60:1481::2000,
            End                  : 2620:0:60:1481::9500,
            PrefixLength         : 64,
            Type                 : 2,
            inUse                : 0,
            Unused               : 29953,
            Pending              : 0,
            Unavailable          : 0
  Subnet 3:
      SubnetAddr      : 2620:0:60:1482::,
      Total           : 1284,
      Static DHCP     : 3,
      Dynamic DHCP    : 1281,
          Ranges:
          Range1:
            Start                : 2620:0:60:1482::1f01,
            End                  : 2620:0:60:1482::1f01,
            PrefixLength         : 64,
            Type                 : 1,
            inUse                : 0,
            Unused               : 1,
            Pending              : 0,
            Unavailable          : 0
          Range2:
            Start                : 2620:0:60:1482::1f02,
            End                  : 2620:0:60:1482::1f02,
            PrefixLength         : 64,
            Type                 : 1,
            inUse                : 0,
            Unused               : 1,
            Pending              : 0,
```

```
          Unavailable           : 0
        Range3:
          Start                 : 2620:0:60:1482::1f03,
          End                   : 2620:0:60:1482::1f03,
          PrefixLength          : 64,
          Type                  : 1,
          inUse                 : 0,
          Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
       Range4:
          Start                 : 2620:0:60:1482::3000,
          End                   : 2620:0:60:1482::3500,
          PrefixLength          : 64,
          Type                  : 2,
         inUse                 : 0,
          Unused                : 1281,
          Pending               : 0,
          Unavailable           : 0
Subnet 4:
  SubnetAddr      : 2620:0:60:1483::,
  Total           : 1284,
  Static DHCP     : 3,
  Dynamic DHCP    : 1281,
      Ranges:
      Range1:
          Start                 : 2620:0:60:1483::1f01,
          End                   : 2620:0:60:1483::1f01,
          PrefixLength          : 64,
          Type                  : 1,
          inUse                 : 0,
          Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
    Range2:
          Start                 : 2620:0:60:1483::1f02,
          End                   : 2620:0:60:1483::1f02,
          PrefixLength          : 64,
          Type                  : 1,
          inUse                 : 0,
          Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
      Range3:
          Start                 : 2620:0:60:1483::1f03,
          End                   : 2620:0:60:1483::1f03,
          PrefixLength          : 64,
          Type                  : 1,
          inUse                 : 0,
          Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
      Range4:
          Start                 : 2620:0:60:1483::4000,
          End                   : 2620:0:60:1483::4500,
          PrefixLength          : 64,
          Type                  : 2,
          inUse                 : 0,
          Unused                : 1281,
```

```
          Pending               : 0,
          Unavailable           : 0

-> show dhcp6-server statistics all
General:
  DHCPv6 Server Name            : DHCPv6,
  DHCPv6 Server Status          : Enabled,
  Total Subnets Managed         : 4,
  Total Subnets Used            : 0,
  Total Subnets Unused          : 4,
  Total Subnets Full            : 0,
  DHCPv6 Server System Up Time  : Mon Jan 12 05:49:54.198,
    Lease DB Sync time (in sec) : 60,
      Last sync time            : Mon Jan 12 08:45:02 2015,
      Next sync time            : Mon Jan 12 08:46:02 2015
Packet:
  Total DHCPv6 Solicts              : 0,
  Total DHCPv6 Advertises           : 0,
  Total DHCPv6 Requests             : 0,
  Total DHCPv6 Renews               : 0,
  Total DHCPv6 Rebinds              : 0,
  Total DHCPv6 Declines             : 0,
  Total DHCPv6 Confirms             : 0,
  Total DHCPv6 Replys               : 0,
  Total DHCPv6 Releases             : 0,
  Total DHCPv6 Information Requests  : 0,
  Total DHCPv6 Lease Querys         : 0,
  Total Delete Leases               : 0,
  Total Unknown packets             : 0
Leases:
    Total:
      Leases Managed            : 50190,
      Leases used               : 0,
      Leases unused             : 50190,
      Leases Pending            : 0,
      Leases unavailable        : 0
    Static DHCPv6:
      Leases Managed            : 10,
      Leases used               : 0,
      Leases unused             : 10,
      Leases Pending            : 0,
      Leases unavailable        : 0
    Dynamic DHCPv6:
      Leases Managed            : 50180,
      Leases used               : 0,
      Leases unused             : 50180,
      Leases Pending            : 0,
      Leases unavailable        : 0
Subnets:
  Subnet 1:
    SubnetAddr      : 2620:0:60:1480::,
    Total           : 17666,
    Static DHCP     : 1,
    Dynamic DHCP    : 17665,
        Ranges:
        Range1:
          Start                 : 2620:0:60:1480::1f01,
          End                   : 2620:0:60:1480::1f01,
          PrefixLength          : 97,
```

```
          Type                  : 1,
          inUse                 : 0,
          Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
        Range2:
          Start                 : 2620:0:60:1480::2000,
          End                   : 2620:0:60:1480::6500,
          PrefixLength          : 97,
          Type                  : 2,
          inUse                 : 0,
          Unused                : 17665,
          Pending               : 0,
          Unavailable           : 0
Subnet 2:
    SubnetAddr      : 2620:0:60:1481::,
    Total           : 29956,
    Static DHCP     : 3,
    Dynamic DHCP    : 29953,
        Ranges:
        Range1:
          Start                 : 2620:0:60:1481::1f01,
          End                   : 2620:0:60:1481::1f01,
          PrefixLength          : 64,
          Type                  : 1,
          inUse                 : 0,
          Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
        Range2:
          Start                 : 2620:0:60:1481::1f02,
          End                   : 2620:0:60:1481::1f02,
          PrefixLength          : 64,
          Type                  : 1,
          inUse                 : 0,
          Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
        Range3:
          Start                 : 2620:0:60:1481::1f03,
          End                   : 2620:0:60:1481::1f03,
          PrefixLength          : 64,
          Type                  : 1,
          inUse                 : 0,
         Unused                : 1,
          Pending               : 0,
          Unavailable           : 0
        Range4:
          Start                 : 2620:0:60:1481::2000,
          End                   : 2620:0:60:1481::9500,
          PrefixLength          : 64,
          Type                  : 2,
          inUse                 : 0,
          Unused                : 29953,
          Pending               : 0,
          Unavailable           : 0
Subnet 3:
    SubnetAddr      : 2620:0:60:1482::,
    Total           : 1284,
```

```
      Static DHCP     : 3,
      Dynamic DHCP    : 1281,
          Ranges:
          Range1:
            Start                 : 2620:0:60:1482::1f01,
            End                   : 2620:0:60:1482::1f01,
            PrefixLength          : 64,
            Type                  : 1,
            inUse                 : 0,
            Unused                : 1,
            Pending               : 0,
            Unavailable           : 0
          Range2:
            Start                 : 2620:0:60:1482::1f02,
            End                   : 2620:0:60:1482::1f02,
            PrefixLength          : 64,
            Type                  : 1,
            inUse                 : 0,
            Unused                : 1,
            Pending               : 0,
            Unavailable           : 0
          Range3:
            Start                 : 2620:0:60:1482::1f03,
            End                   : 2620:0:60:1482::1f03,
            PrefixLength          : 64,
            Type                  : 1,
            inUse                 : 0,
            Unused                : 1,
            Pending               : 0,
            Unavailable           : 0
          Range4:
            Start                 : 2620:0:60:1482::3000,
            End                   : 2620:0:60:1482::3500,
            PrefixLength          : 64,
            Type                  : 2,
            inUse                 : 0,
            Unused                : 1281,
            Pending               : 0,
            Unavailable           : 0
  Subnet 4:
      SubnetAddr      : 2620:0:60:1483::,
      Total           : 1284,
      Static DHCP     : 3,
      Dynamic DHCP    : 1281,
          Ranges:
          Range1:
            Start                 : 2620:0:60:1483::1f01,
            End                   : 2620:0:60:1483::1f01,
            PrefixLength          : 64,
            Type                  : 1,
            inUse                 : 0,
            Unused                : 1,
            Pending               : 0,
            Unavailable           : 0
          Range2:
            Start                 : 2620:0:60:1483::1f02,
            End                   : 2620:0:60:1483::1f02,
            PrefixLength          : 64,
            Type                  : 1,
```

```
    inUse                : 0,
    Unused               : 1,
    Pending              : 0,
    Unavailable          : 0
  Range3:
    Start                : 2620:0:60:1483::1f03,
    End                  : 2620:0:60:1483::1f03,
    PrefixLength         : 64,
    Type                 : 1,
    inUse                : 0,
    Unused               : 1,
    Pending              : 0,
    Unavailable          : 0
  Range4:
    Start                : 2620:0:60:1483::4000,
    End                  : 2620:0:60:1483::4500,
    PrefixLength         : 64,
    Type                 : 2,
    inUse                : 0,
    Unused               : 1281,
    Pending              : 0,
    Unavailable          : 0
```

output definitions

General	Denotes general DHCPv6 Server statistics.
DHCPv6 Server Name	Specifies the name assigned to the DHCPv6 server.
DHCPv6 Server Status	Specifies up or down status of the DHCPv6 server.
Total subnets used	Specifies the total number of subnets being used.
Total subnets managed	Specifies the total number of subnets being managed by the DHCPv6 server.
Total subnets unused	Specifies the total number of subnets being unused.
Total subnets full	Specifies the total number of subnets where all the IP addresses are used.
DHCP Server System Up Time	Shows the DHCPv6 Server System Up Time Performance Monitor counter.
Sync time	Specifies the time for DHCPv6 server to contact and synchronize with the designated time server.
Last sync time	Specifies the last time the synchronization occurred.
Next sync time	Specifies the next time the synchronization should be scheduled.
Packet stats	Denotes statistical information about the data packet transmission.
Total DHCP Discovers	Specifies the total number of DHCPDISCOVER packets sent by the clients to the DHCPv6 server.
Total DHCP Offers	Specifies the total number of DHCPOFFER packets sent by the server to the clients.
Total DHCP Requests	Specifies the total number of DHCPREQUEST packets sent by the clients in response to the DHCPOFFER packets.
Total DHCP Request Grants	Specifies the total number of DHCPv6 request grants provided by the server to the clients.

output definitions (continued)

Total DHCP Request Renews	Specifies the total number of DHCPv6 lease renew requests sent by the clients to the DHCPv6 server.
Total DHCP Declines	Specifies the total number of DHCPv6 requests declined by the DHCPv6 server.
Total DHCP Acks	Specifies the total number of DHCPACK acknowledgement packets sent by the DHCPv6 server to the clients.
Total DHCP Nacks	Specifies the total number of DHCPv6 Negative acknowledgements sent from the DHCPv6 server to the clients. The DHCPNACK message is sent when all the IP addresses available to the server are exhausted and the client sends a DHCPREQUEST.
Total DHCP Releases	Specifies the total number of DHCPRELEASE packets sent by the DHCPv6 server to release IP addresses from its clients.
Total DHCP Informs	Specifies the total number of DHCPINFORM packets sent by the clients to obtain DHCPv6 options from the DHCPv6 server.
Total Bootp requests	Specifies the total number of BOOTP requests sent by the clients to the DHCPv6 server.
Total Bootp response	Specifies the total number of BOOTP response packets sent by the DHCPv6 server to the clients.
Total Unknown packets	Specifies the total number of unknown or badly formatted DHCPv6 packets received by the DHCPv6 server.
Leases stats	Denotes statistical information about leases provided by the DHCPv6 server.
Hosts Managed	Specifies the total number of clients managed by the DHCPv6 server.
Hosts used	Specifies the total number of clients using the IP addresses provided by the DHCPv6 server.
Hosts unused	Specifies the total number of clients managed by the DHCPv6 server which are not being used.
Hosts Pending	Specifies the total number of DHCPv6 IP address requests which are pending by the DHCPv6 server.
Hosts unavailable	Specifies the total number of DHCPv6 hosts which are unavailable (for example, hosts whose lease period has expired).
Static DHCP	Denotes statistical information about the hosts configured with Static DHCPv6.
Automatic DHCP	Denotes statistical information about the hosts configured with Automatic DHCPv6.
Static BootP	Denotes statistical information about the hosts configured under Static BootP. **Note:** BootP Relay is disabled when DHCPv6 server is enabled on the switch.
Automatic BootP	Denotes statistical information about the hosts configured with Automatic BootP.
Subnet statistics	Denotes all DHCPv6 related statistical information for individual subnets.
Range	Specifies the range of IP addresses in the individual subnet.

output definitions (continued)

Mask	Specifies the subnet mask.
Type	Specifies whether the type of IP address allocation is dynamic or static.

Release History

Release 7.3.4; command introduced.

Related Commands

clear dhcpv6-server statistics	Clears the DHCPv6 Server lease statistics.

MIB Objects

N/A

clear dhcpv6-server statistics

Clears the packet counters of DHCPv6 server statistics.

clear dhcpv6-server statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

Use this command to clear the packet counters of DHCPv6 server statistics.

Examples

```
-> clear dhcpv6-server statistics
```

Release History

Release 7.3.4; command introduced.

Related Commands

show dhcpv6-server statistics	Displays the DHCPv6 Server lease statistics.

MIB Objects

N/A

dhcp-message-service

Enable or disable the message service operation.

dhcp-message-service {enable | disable}

Syntax Definitions

enable	Enables the operational status of the message service.
disable	Disables the operational status of the message service.

Defaults

By default, the operational status of the message service is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **conf** and **pcy** files are parsed when message service is enabled.
- There is one instance of the message service for the default VRF in the switch that can be enabled or disabled.

Examples

```
-> dhcp-message-service enable
-> dhcp-message-service disable
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-message-service restart	Restarts the message service after the msgd.conf file is modified.

MIB Objects

```
alaMsgSrvGlobalConfigStatus
```

dhcp-message-service restart

Restarts the message service after the **msgd.conf** file or **dhcpd.pcy** is modified.

dhcp-message-service restart

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Before using this command, enable the message service status using the **dhcp-message-service** command.

Examples

```
-> message-service restart
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-message-service	Enable or disable the message service operation.

MIB Objects

```
alaMsgSrvGlobalRestart
```

show message-service status

Displays the status and statistical information related to the message service running on the switch.

show message-service status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show message-service status
Message Service is enabled
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-message-service	Enable or disable the message service operation.
dhcp-message-service restart	Restarts the message service, after the msgd.conf file is modified.

MIB Objects

N/A

active-lease-service

Enable or disable the Active Lease Service operation.

active-lease-service {enable | disable}

Syntax Definitions

enable	Enables the operational status of the Active Lease Service.
disable	Disables the operational status of the Active Lease Service.

Defaults

By default, the operational status of Active Lease Service is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

There is one instance of Active Lease Service for the default VRF in the switch that can be enabled or disabled.

Examples

```
-> active-lease-service enable
-> active-lease-service disable
```

Release History

Release 7.3.4; command introduced.

Related Commands

active-lease-service restart	Restarts the Active Lease Service after the netd.pcy file is modified.
show active-lease-service status	Displays the status and statistical information related to Active Lease Service running on the switch.

MIB Objects

```
alaActiveLeaseSrvGlobalConfigStatus
```

active-lease-service restart

Restarts the Active Lease Service after the netd.pcy file is modified.

active-lease-service restart

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Before using this command, enable the Active Lease Service using the **active-lease-service** command.

Examples

```
-> active-lease-service restart
```

Release History

Release 7.3.4; command introduced.

Related Commands

active-lease-service	Enable or disable the Active Lease Service operation.
show active-lease-service status	Displays the status and statistical information related to Active Lease Service running on the switch.

MIB Objects

```
alaActiveLeaseSrvGlobalRestart
```

show active-lease-service status

Displays the status and statistical information related to the Active Lease Service running on the switch.

show active-lease-service status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show active-lease-service status
Active Lease Service is enabled
```

Release History

Release 7.3.4; command introduced.

Related Commands

active-lease-service	Enable or disable the Active Lease Service operation.

MIB Objects

N/A

dhcp-snooping admin-state

Enables or disables DHCP Snooping for the switch.

dhcp-snooping admin-state {enable | disable}

no dhcp-snooping

Syntax Definitions

enable	Enables DHCP Snooping for the switch.
disable	Disables DHCP Snooping for the switch.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When DHCP Snooping is administratively disabled for the switch, the DHCP Snooping configuration remains and dynamic binding table entries are cleared.
- When the **no** form of the command is used, the DHCP Snooping configuration is *removed* and dynamic binding table entries are cleared.

Examples

```
-> dhcp-snooping admin-state enable
-> dhcp-snooping admin-state disable
-> no dhcp-snooping
```

Release History

Release 7.3.4; command introduced.
Release 8.6R1; **no** form of the command added.

Related Commands

dhcp-snooping vlan	.Enables or disables DHCP Snooping on a per-VLAN basis.
show dhcp-snooping	Displays the current DHCP Snooping configuration for the switch.

MIB Objects

`dhcpSnoopingMode`

dhcp-snooping mac-address-verification

Globally enables or disables MAC address verification for incoming DHCP traffic. When this feature is enabled, the source MAC address is compared to the client hardware MAC address in the DHCP packet. If these two addresses do not match, the DHCP packet is dropped.

dhcp-snooping mac-address-verification admin-state {enable | disable}

Syntax Definitions

enable	Enables DHCP MAC address verification for the switch.
disable	Disables DHCP MAC address verification for the switch.

Defaults

By default, this feature is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- DHCP Snooping must be enabled before using this command.
- When DHCP Snooping is enabled at the switch level, MAC address verification and Option-82 data insertion are enabled by default. In addition, the trust mode for all ports is set to the DHCP client only mode.
- Changing the enabled or disabled status for MAC address verification is only allowed when DHCP Snooping is globally enabled for the switch.

Examples

```
-> dhcp-snooping mac-address-verification admin-state enable
-> dhcp-snooping mac-address-verification admin-state disable
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping admin-state	.Globally enables or disables DHCP Snooping for the switch.
dhcp-snooping option-82-data-insertion	Globally enables or disables DHCP Option-82 data insertion for DHCP packets.
show dhcp-snooping	Displays the current DHCP Snooping configuration for the switch.

MIB Objects

```
dhcpSnoopingMacAddrVerificationStatus
```

dhcp-snooping option-82-data-insertion

Globally enables or disables DHCP Option-82 data insertion for DHCP packets. When this feature is enabled, the relay agent inserts the Option-82 field into DHCP packets before forwarding them to the DHCP server.

dhcp-snooping option-82-data-insertion admin-state {enable | disable}

Syntax Definitions

enable	Enables inserting the DHCP Option-82 field into DHCP packets.
disable	Disables inserting the DHCP Option-82 field into DHCP packets.

Defaults

By default, this feature is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- DHCP Snooping must be enabled before using this command.
- When DHCP Snooping is enabled at the switch level, Option-82-data-insertion and MAC address verification are enabled by default. In addition, the trust mode for all ports is set to the DHCP client only mode.

Examples

```
-> dhcp-snooping option-82-data-insertion admin-state enable
-> dhcp-snooping option-82-data-insertion admin-state disable
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping admin-state	.Globally enables or disables DHCP Snooping for the switch.
dhcp-snooping option-82 format	Configures the type of information that is inserted in both the Circuit ID and Remote ID suboption of the Option-82 field.
show dhcp-snooping	Displays the current DHCP Snooping configuration for the switch.

MIB Objects

```
dhcpSnoopingOpt82DataInsertionStatus
```

dhcp-snooping bypass option-82-check

Enables or disables checking for an Option-82 field in DHCP packets ingressing on untrusted ports.

dhcp-snooping bypass option-82-check admin-state {enable | disable}

Syntax Definitions

enable	Bypasses the Option-82 field check.
disable	Checks DHCP packets for the Option-82 field.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When this feature is disabled (the default), DHCP packets ingressing on untrusted ports are checked to see if they contain the Option-82 field. If this field is present, the DHCP packet is discarded.
- When this feature is enabled, DHCP packets ingressing on untrusted ports are *not* checked to see if they contain the Option-82 field. In this case, the Option-82 field is ignored and all DHCP packets are processed.
- Using this command is only allowed when DHCP Snooping is enabled globally for the switch or at the VLAN level.

Examples

```
-> dhcp-snooping bypass option-82-check admin-state enable
-> dhcp-snooping bypass option-82-check admin-state disable
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping admin-state	Globally enables or disables DHCP Snooping for the switch.
show dhcp-snooping	Displays the current DHCP Snooping configuration for the switch.

MIB Objects

```
dhcpSnoopingBypassOpt82CheckStatus
```

dhcp-snooping option-82 format

Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.

dhcp-snooping option-82 format [base-mac | system-name | user-string *string* | **interface-alias | auto-interface-alias | ascii [{ remote-id | circuit-id} {base-mac | cvlan | interface | interface-alias | system-name | user-string** *string* **| vlan} {delimiter** *string***}]]**

no dhcp-snooping option-82 format ascii {remote-id | circuit-id}

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The system name of the switch.
string	A user defined text string. Supports up to 64 characters.
interface-alias	The alias configured for the interface.
auto-interface-alias	The switch automatically generates the interface-alias in the following format: SystemName_slot_port. ascii ASCII format.
ascii	ASCII format. **remote-id** | **circuit-id**: Select the sub-id fields of option-82 to configure ASCII. **base-mac**: The base MAC address of the switch. **cvlan**: The Customer VLAN ID. **interface**: The interface name. **interface-alias**: The alias configured for the interface. **system-name**: The system name of the switch. **user-string**: A user defined text string. **vlan**: The VLAN ID of which the client is a member. string: A user-defined text string. **delimiter**: The delimiter character that separates fields within the Circuit ID and Remote ID ASCII string value. Valid characters are | (pipe), \ (backward slash), / (forward slash), - (dash), _ (underscore), and " " (space).

Defaults

parameter	default
user-string *string* | system-name | interface-alias | base-mac | auto-interface-alias | ascii	base-mac
ascii	base-mac

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The string parameter specifies user-defined information to insert into the Circuit ID and Remote ID fields.
- When entering a string for user-defined Option-82 information, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the string “Building B Server” requires quotes because of the spaces between the words.
- The interface-alias parameter will use the alias configured with the interfaces alias command. If no alias is configured a NULL string will be inserted.
- A maximum of 63 characters can be inserted when using the interface-alias and auto-interface-alias commands, remaining characters will be truncated.
- The Option-82 format option is a global setting, the format specified will be applied to all ports on the switch.
- The data specified with this command is added to the Circuit ID and Remote ID fields only when DHCP Option-82 data insertion is enabled for the switch.
- When DHCP Snooping is enabled at the switch level, Option-82 data insertion is enabled by default.
- The ASCII option is used to specify the type of information that is configured in ASCII text string format and then inserted into the Option-82 Circuit ID suboption. Each parameter provided with this command represents a different type of information.
- Configuring the Circuit ID or Remote ID suboption in ASCII format allows up to five fields (types) of information within the ASCII string. However, if the contents of all the fields combined exceeds 127 characters, then the ASCII string is truncated.
- Specifying at least one parameter with ASCII option is required. If multiple parameters are selected, then specifying one of the valid delimiter characters is also required.
- In order for the backward slash “\” delimiter to be parsed correctly it must be entered as “\\”.
- Use the **no** form of this command to remove the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 fields option-82-check admin-state disable.

Examples

```
-> dhcp-snooping option-82 format user-string “Building B Server”
-> dhcp-snooping option-82 format system-name
-> dhcp-snooping option-82 format base-mac
-> dhcp-snooping option-82 format interface-alias
-> dhcp-snooping option-82 format auto-interface-alias
-> no dhcp-snooping option-82 format ascii remote-id
-> no dhcp-snooping option-82 format ascii circuit-id
-> dhcp-snooping option-82 format ascii circuit-id cvlan cvlan delimiter “\\”
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping option-82-data-insertion	Globally enables or disables DHCP Option-82 data insertion for DHCP packets.
dhcp-snooping admin-state	Globally enables or disables DHCP Snooping for the switch
show dhcp-snooping	Displays the current DHCP Snooping configuration for the switch.

MIB Objects

```
dhcpSnoopingOption82FormatType
dhcpSnoopingOption82StringValue
dhcpSnoopingOption82FormatASCIIConfigurableEntry
dhcpSnoopingOption82FormatASCIIConfigurableIndex
dhcpSnoopingOption82FormatASCIIConfigurableField1
dhcpSnoopingOption82FormatASCIIConfigurableField1StrVal
dhcpSnoopingOption82FormatASCIIConfigurableField2
dhcpSnoopingOption82FormatASCIIConfigurableField2StrVal
dhcpSnoopingOption82FormatASCIIConfigurableField3
dhcpSnoopingOption82FormatASCIIConfigurableField3StrVal
dhcpSnoopingOption82FormatASCIIConfigurableField4
dhcpSnoopingOption82FormatASCIIConfigurableField4StrVal
dhcpSnoopingOption82FormatASCIIConfigurableField5
dhcpSnoopingOption82FormatASCIIConfigurableField5StrVal
dhcpSnoopingOption82FormatASCIIConfigurableDelimiter
```

dhcp-snooping option-82 policy

Specifies whether to keep, replace, or drop the Option-82 field from DHCP packets entering the switch.

dhcp-snooping option-82 policy [replace | keep | drop]

Syntax Definitions

replace	Replaces Option-82 field in the incoming DHCP packets.
keep	Keeps Option-82 field in the incoming DHCP packets.
drop	Drops the packet with Option-82 in the incoming DHCP packets.

Defaults

By default, the Option-82 field is replaced in the DHCP packets.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> dhcp-snooping option-82 policy replace
-> dhcp-snooping option-82 policy keep
-> dhcp-snooping option-82 policy drop
```

Release History

Release 8.5R2; command introduced.

Related Commands

dhcp-snooping admin-state	Globally enables or disables DHCP Snooping for the switch.
show dhcp-snooping	Displays the global DHCP Snooping configuration.

MIB Objects

```
dhcpSnoopingOption82Policy
```

dhcp-snooping vlan

Enables or disables DHCP Snooping on a per VLAN basis. When this feature is enabled, all DHCP packets received on ports associated with the DHCP Snooping VLAN are filtered.

dhcp-snooping vlan *vlan_id***[-***vlan_id2***] [mac-address-verification | option-82-data-insertion] admin-state {enable | disable}**

no dhcp-snooping vlan *vlan_id***[-***vlan_id2***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	The VLAN identification number. Valid range is 1–4094. Use a hyphen to specify a range of VLANs (10-15).
mac-address verification	Enables or disables verifying the source MAC address of DHCP packets with the client MAC address contained in the same packet.
option-82 data-insertion	Enables or disables inserting Option-82 information into DHCP packets.
admin-state	Enables or disables DHCP snooping feature for specified VLAN.

Defaults

By default, DHCP Snooping is disabled. When this feature is enabled for the specified VLAN, the following default parameter values apply:

parameter	default
mac-address verification	Enabled
option-82 data-insertion	Enabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the DHCP Snooping configuration for the specified VLAN.
- The MAC address verification and Option-82 data insertion are applied to packets received on ports associated with the DHCP Snooping VLAN.
- If the DHCP relay agent Option-82 feature is enabled, DHCP Snooping is not available. These two features are mutually exclusive.
- If the DHCP Snooping feature is globally enabled for the switch, then configuring snooping on a per-VLAN basis is not allowed. The opposite is also true; invoking VLAN based snooping prevents the use of switch level snooping.

- Note that disabling the DHCP Snooping Option-82 data insertion operation for a VLAN is not allowed when the binding table functionality is enabled.

Examples

```
-> dhcp-snooping vlan 100 admin-state enable
-> dhcp-snooping vlan 100 admin-state disable
-> dhcp-snooping vlan 100 mac-address-verification admin-state enable
-> no dhcp-snooping vlan 100
-> dhcp-snooping vlan 200-205 admin-state enable
-> dhcp-snooping vlan 200-205 admin-state disable
-> dhcp-snooping vlan 200-205 option-82 data-insertion admin-state enable
-> no dhcp-snooping vlan 200-205
```

Release History

Release 7.3.4; command introduced.
Release 8.6R1; **no** form of the command added.

Related Commands

dhcp-snooping admin-state	Globally enables or disables DHCP Snooping for the switch.
show dhcp-snooping vlan	Displays a list of DHCP Snooping VLANs.

MIB Objects

```
dhcpSnoopingVlanTable
   dhcpSnoopingVlanNumber
   dhcpSnoopingVlanMacAddrVerificationStatus
   dhcpSnoopingVlanOpt82DataInsertionStatus
   dhcpSnoopingVlanStatus
   dhcpSnoopingVlanAdminState
```

dhcp-snooping port

Configures the DHCP Snooping trust mode for the port. The trust mode determines if the port will accept all DHCP traffic, block all DHCP traffic, or accept only client DHCP traffic.

dhcp-snooping port *chassis*/*slot1*/*port***[-***port2***] {block | client-only | trust}**

Syntax Definitions

chassis	The chassis identifier.
slot1/*port***[-***port2***]**	The slot and port number (1/1/3). Use a hyphen to specify a range of ports (1/1/3-8).
block	Blocks all DHCP traffic on the port.
client-only	Allows only DHCP client traffic on the port.
trust	Allows all DHCP traffic on the port. The port behaves as if DHCP Snooping was not enabled.

Defaults

By default, the trust mode for a port is set to **client-only** when the DHCP Snooping feature is enabled for the switch or for a VLAN.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The DHCP trust mode only applies when the DHCP Snooping feature is enabled for the switch or for a VLAN.
- If DHCP Snooping is enabled at the switch level, the trust mode applies to all switch ports.
- If DHCP Snooping is enabled for a specific VLAN, then the trust mode applies to only those ports that are associated with that VLAN.

Examples

```
-> dhcp-snooping port 1/1/24 trust
-> dhcp-snooping port 1/1/1-10 block
-> dhcp-snooping port 1/1/8 client-only
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping admin-state	Globally enables or disables DHCP Snooping for the switch.
dhcp-snooping vlan	Enables or disables DHCP Snooping on a per-VLAN basis.
show dhcp-snooping port	Displays the current trust mode for a port and statistics regarding the number of packets dropped due to DHCP Snooping violations

MIB Objects

```
dhcpSnoopingPortTable
   dhcpSnoopingPortIfIndex
   dhcpSnoopingPortTrustMode
```

dhcp-snooping linkagg

Configures the DHCP Snooping trust mode for the link aggregate. The trust mode determines if the link aggregate will accept all DHCP traffic, block all DHCP traffic, or accept only client DHCP traffic.

dhcp-snooping linkagg *agg_id***[-***agg_id2***] {block | client-only | trust}**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (1-5).
block	Blocks all DHCP traffic on the link aggregate.
client-only	Allows only DHCP client traffic on the link aggregate.
trust	Allows all DHCP traffic on the link aggregate. The link aggregate behaves as if DHCP Snooping was not enabled.

Defaults

By default, the trust mode for a link aggregate is set to **client-only** when the DHCP Snooping feature is enabled for the switch or for a VLAN.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The DHCP trust mode only applies when the DHCP Snooping feature is enabled for the switch or for a VLAN.
- If DHCP Snooping is enabled at the switch level, the trust mode applies to all link aggregates.
- If DHCP Snooping is enabled for a specific VLAN, then the trust mode applies to only those link aggregates that are associated with that VLAN.
- Use the **show dhcp-snooping port** command to display the current trust mode for a link aggregate and statistics regarding the number of packets dropped due to DHCP Snooping violations.

Examples

```
-> dhcp-snooping linkagg 1 trust
-> dhcp-snooping linkagg 5-8 trust
-> dhcp-snooping linkagg 2 block
-> dhcp-snooping linkagg 5-8 block
-> dhcp-snooping linkagg 3 client-only
-> dhcp-snooping linkagg 5-8 client-only
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping admin-state	Globally enables or disables DHCP Snooping for the switch.
dhcp-snooping vlan	Enables or disables DHCP Snooping on a per-VLAN basis.

MIB Objects

```
dhcpSnoopingPortTable
   dhcpSnoopingPortIfIndex
   dhcpSnoopingPortTrustMode
```

dhcp-snooping ip-source-filter admin-state

Enables or disables the DHCP Snooping IP source filtering functionality for the switch.

dhcp-snooping ip-source-filtering admin-state {enable | disable}

Syntax Definitions

enable	Enables IP source filtering for the switch.
disable	Disables IP source filtering for the switch.

Defaults

By default, the DHCP Snooping IP source filtering functionality is enabled for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When IP source filtering is disabled for the switch, the user-defined IP source filtering configuration is maintained but not operationally active.
- When DHCP Snooping is disabled for the switch, the status of IP source filtering is not changed; if IP source filtering is enabled, the functionality is still applied to static binding table entries.

Examples

```
-> dhcp-snooping ip-source-filter admin-state disable
-> dhcp-snooping ip-source-filter admin-state enable
```

Release History

Release 8.6R1; command introduced.

Related Commands

dhcp-snooping ip-source-filter	Enables or disables DHCP Snooping IP source filtering for a port, link aggregate, or VLAN.
show dhcp-snooping ip-source-filter	Displays the global IP source filtering status.

MIB Objects

`dhcpSnoopingIpSourceFilterAdminState`

dhcp-snooping ip-source-filter

Enables or disables the IP source filtering capability on a port, link aggregate, or VLAN. When this function is enabled, the switch allows the traffic that matches the client IP address, MAC address, port, and VLAN combination obtained from the DHCP snooping binding table entry.

dhcp-snooping ip-source-filter {vlan *vlan_id***[-***vlan_id2***]| port** *chassis*/*slot*/*port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} admin-state {enable | disable}**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	The VLAN identification number (1–4094). Use a hyphen to specify a range of VLANs (10-15).
chassis	The chassis identifier.
slot1/*port***[-***port2***]**	The slot and port number (1/1/3). Use a hyphen to specify a range of ports (1/1/3-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (1-5).
enable	Enables IP source filtering for the specified port, link aggregate, or VLAN.
disable	Disables IP source filtering for the specified port, link aggregate, or VLAN level.

Defaults

By default, IP source filtering is disabled for a port, link aggregate, or VLAN.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Source filtering can be enabled only on the VLANs on which the DHCP Snooping is enabled.
- Source filtering can be enabled as follows:
  - on the ports that are associated with a VLAN on which DHCP Snooping is enabled.
  - on all the ports when DHCP Snooping is globally enabled for the switch.
- The user-defined IP source filtering configuration is not operationally active unless the IP source filtering functionality is globally enabled for the switch. By default, the global functionality is enabled and is configurable through the **dhcp-snooping ip-source-filter admin-state** command.

Examples

```
-> dhcp-snooping ip-source-filter port 1/1/1 admin-state enable
-> dhcp-snooping ip-source-filter port 1/1/1-5 admin-state enable
-> dhcp-snooping ip-source-filter linkagg 2 admin-state enable
-> dhcp-snooping ip-source-filter vlan 10 admin-state enable
-> dhcp-snooping ip-source-filter vlan 20 admin-state disable
```

Release History

Release 7.3.4; command introduced.
Release 8.5R2; support for port ranges added.

Related Commands

dhcp-snooping ip-source-filter admin-state	Enables or disables DHCP Snooping IP source filtering functionality for the switch.
show dhcp-snooping ip-source-filter	Displays the ports or VLANs on which IP source filtering is enabled.

MIB Objects

```
dhcpSnoopingSourceFilterVlanTable
   dhcpSnoopingSourceFilterVlanNumber
   dhcpSnoopingSourceFilterVlanFilteringStatus
dhcpSnoopingPortTable
   dhcpSnoopingPortIpSourceFiltering
```

dhcp-snooping binding admin-state

Enables or disables the DHCP Snooping binding table functionality. The binding table contains the MAC address, IP address, lease time, binding type (dynamic or static), VLAN number, and the interface information that corresponds to a local untrusted port on the switch.

dhcp-snooping binding admin-state {enable | disable}

Syntax Definitions

enable	Enables the creation of binding table entries.
disable	Disables the creation of binding table entries.

Defaults

By default, the binding table functionality is enabled when the DHCP Snooping feature is enabled for the switch or for a VLAN.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Note that enabling the binding table functionality is not allowed if Option-82 data insertion is *not* enabled at either the switch or VLAN level.

Examples

```
-> dhcp-snooping binding admin-state disable
-> dhcp-snooping binding admin-state enable
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.
dhcp-snooping binding action	Synchronizes the contents of the DHCP Snooping binding table with the contents of the **dhcpBinding.db** file saved on the switch.

MIB Objects

```
dhcpSnoopingBindingStatus
```

dhcp-snooping binding timeout

Configures the amount of time between each automatic save of the DHCP Snooping binding table contents maintained in memory to a file on the switch. This functionality preserves binding table contents across switch reboots.

dhcp-snooping binding timeout *seconds*

Syntax Definitions

seconds	The number of seconds to wait before the next save. The valid range is 1–600.

Defaults

By default, the timeout value is set to 1 second.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The timeout value is only valid if the DHCP Snooping binding table functionality is enabled.
- The contents of the binding table is saved to the **dhcpBinding.db** file in the **/flash/switch** directory.
- The **dhcpBinding.db** file is time stamped when a save of the binding table contents is successfully completed.

Examples

```
-> dhcp-snooping binding timeout 600
-> dhcp-snooping binding timeout 250
```

Release History

Release 7.3.4; command introduced.
Release 8.6R1; default timeout changed to 1 second and valid timeout range changed to 1–600 seconds.

Related Commands

dhcp-snooping binding admin-state	.Enables or disables the DHCP Snooping binding table functionality.
dhcp-snooping binding action	Synchronizes the contents of the DHCP Snooping binding table with the contents of the **dhcpBinding.db** file saved on the switch.

MIB Objects

```
dhcpSnoopingBindingDatabaseSyncTimeout
```

dhcp-snooping binding action

Triggers a purge, renew, or save action against the DHCP Snooping binding table. A purge action clears the contents of the table. A renew action populates the table with entries saved in the **dhcpBinding.db** file. A save action saves table entries in switch memory to the **dhcpBinding.db** file.

dhcp-snooping binding action {purge | renew | save}

Syntax Definitions

purge	Clears all binding table entries that are maintained in switch memory.
renew	Populates the binding table with entries saved in the **dhcpBinding.db file** located in the **/flash/switch** directory on the switch.
save	Saves the binding table entries in switch memory to the **dhcpBinding.db file** located in the **/flash/switch** directory on the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The DHCP Snooping binding table is maintained in the switch memory. Binding table entries are saved on a periodic basis to the **dhcpBinding.db** file on the switch. Use the **save** option to invoke an explicit save of binding table entries to the **dhcpBinding.db** file.
- To sync the binding table contents with the contents of the **dhcpBinding.db** file:
  - use the **purge** option to clear the binding table entries, then
  - use the **renew** option to repopulate the binding table with entries saved in the **dhcpBinding.db** file.

Examples

```
-> dhcp-snooping binding action purge
-> dhcp-snooping binding action renew
-> dhcp-snooping binding action save
```

Release History

Release 7.3.4; command introduced.
Release 8.6.R1; **save** option added.

Related Commands

dhcp-snooping binding admin-state	.Enables or disables the DHCP Snooping binding table functionality.
dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.

MIB Objects

```
dhcpSnoopingBindingDatabaseAction
```

dhcp-snooping binding persistency

Retains the entries in the DHCP Snooping binding table for the duration of the lease regardless of the existence of the MAC address in the MAC address table.

dhcp-snooping binding persistency admin-state {enable | disable}

Syntax Definitions

enable	Enables DHCP Snooping binding persistency.
disable	Disables DHCP Snooping binding persistency.

Defaults

By default, DHCP Snooping binding persistency is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- With this option disabled, the entry will be removed if the MAC address is missing from the MAC address table when the database is synchronized.
- Use the **show dhcp-snooping** command to display the current status.

Examples

```
-> dhcp-snooping binding persistency admin-state enable
-> dhcp-snooping binding persistency admin-state disable
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping binding admin-state	Enables or disables the DHCP Snooping binding table functionality.
dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.

MIB Objects

```
dhcpSnoopingBindingPersistencyStatus
```

dhcp-snooping binding

Creates a static entry in the binding table.

dhcp-snooping binding *mac_address* **port** *chassis/slot/port* **address** *ip_address* **vlan** *vlan_id*

no dhcp-snooping binding *mac_address* **port** *chassis/slot/port* **address** *ip_address* **vlan** *vlan_id*

Syntax Definitions

mac_address	The client MAC address.
chassis	The chassis identifier.
*slot1/port***[**-*port2***]**	The slot and port number (3/1).
ip_address	The IP address that the DHCP server offered to the client.
vlan_id	The VLAN identification number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Static binding table entries are created using this command. If DHCP Snooping binding table functionality is not enabled, creating a static entry is not allowed.
- Dynamic binding table entries are created when the relay agent receives a DHCPACK packet.
- Use the **no** form of this command to remove a static entry from the DHCP Snooping binding table.

Examples

```
-> dhcp-snooping binding 00:2a:95:51:6c:10 port 1/1/15 address 17.15.3.10 vlan 200
-> no dhcp-snooping binding 00:2a:95:51:6c:10 port 1/1/15 address 17.15.3.10 vlan
200
```

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.
dhcp-snooping binding action	Synchronizes the contents of the DHCP Snooping binding table with the contents of the **dhcpBinding.db** file saved on the switch.
show dhcp-snooping binding	Displays the contents of the DHCP Snooping binding table (database).

MIB Objects

```
dhcpSnoopingBindingTable
   dhcpSnoopingBindingMacAddress
   dhcpSnoopingBindingIfIndex
   dhcpSnoopingBindingIpAddress
   dhcpSnoopingBindingVlan
   dhcpSnoopingBindingRowStatus
```

show dhcp-snooping

Displays the global DHCP Snooping configuration.

show dhcp-snooping

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When DHCP Snooping is enabled for the switch or for a specific VLAN, the DHCP Snooping binding database status is automatically enabled and additional fields are displayed.
- When DHCP Snooping is enabled at the switch level, the “Option 82 Data Insertion Per Switch” and “MAC Address Verification Per Switch” fields are displayed; these fields do not display when DHCP Snooping is enabled at the VLAN level.

Examples

```
-> show dhcp-snooping
DHCP Snooping :
  DHCP Snooping Status                              =  Disabled
  DHCP Snooping Bypass Opt82-Check                  =  Disabled,
  DHCP Snooping Opt82 Format                        =  Base MAC,
  DHCP Snooping Opt82 String                        =  2c:fa:a2:13:e4:02,
  DHCP Snooping Binding DB Status                   =  Disabled,
  DHCP Snooping Option-82 Policy                    =  Replace,

-> dhcp-snooping admin-state enable
-> show dhcp-snooping
DHCP Snooping :
  DHCP Snooping Status                              =  Switch-Level Enabled,
      Option 82 Data Insertion Per Switch           =  Enabled,
      MAC Address Verification Per Switch           =  Enabled,
  DHCP Snooping Bypass Opt82-Check                  =  Disabled,
  DHCP Snooping Opt82 Format                        =  Base MAC,
  DHCP Snooping Opt82 String                        =  2c:fa:a2:13:e4:02,
  DHCP Snooping Binding DB Status                   =  Enabled,
      Database Sync Timeout                         =  1,
      Database Last Sync Time                       =  Oct 25 2016 14:56,
      Binding Persistency Status                    =  Disabled,
  DHCP Snooping Option-82 Policy                    =  Replace,

-> dhcp-snooping vlan 200 admin-state enable
-> show dhcp-snooping
```

```
DHCP Snooping :
  DHCP Snooping Status                              =  VLAN-Level,
  DHCP Snooping Bypass Opt82-Check                  =  Disabled,
  DHCP Snooping Opt82 Format                        =  Base MAC,
  DHCP Snooping Opt82 String                        =  2c:fa:a2:13:e4:02,
  DHCP Snooping Binding DB Status                   =  Enabled,
      Database Sync Timeout                         =  1,
      Database Last Sync Time                       =  Oct 28 2016 07:36,
      Binding Persistency Status                    =  Disabled,
  DHCP Snooping Option-82 Policy                    =  Replace,
```

output definitions

DHCP Snooping Status	Displays whether DHCP Snooping is enabled at the **Switch-Level**, **VLAN-Level**, or **Disabled**.
Option 82 Data Insertion Per Switch	Indicates whether or not (**Enabled** or **Disabled**) the relay agent inserts the Option-82 field into DHCP packets before forwarding them to the DHCP server. Configured through the **dhcp-snooping option-82-data-insertion** command.
MAC Address Verification Per Switch	Indicates whether or not (**Enabled** or **Disabled**) the source MAC address is compared to the client hardware MAC address in the DHCP packet; if there is a mismatch the packet is dropped. Configured through the **dhcp-snooping mac-address-verification**
DHCP Snooping Bypass Opt82-Check	Indicates whether DHCP packets received on untrusted ports are checked to see if they contain the Option-82 field (**Disabled**) or not checked (**Enabled**). Configured through the **dhcp-snooping bypass option-82-check** command.
DHCP Snooping Opt82 Format	Displays the type of Option-82 information inserted into the Circuit ID and Remote ID suboptions of the Option-82 field. Configured through the **dhcp-snooping option-82 format** command.
DHCP Snooping Opt82 string	Displays the contents of the Option-82 string that is inserted into the Circuit ID and Remote ID supoptions of the Option-82 field.
DHCP Snooping Binding DB Status	Displays whether the DHCP Snooping binding table functionality is **Enabled** or **Disabled**. Configured through the **dhcp-snooping binding admin-state** command.
Database Sync Timeout	The amount of time, in seconds, between each automatic save of the DHCP Snooping binding table contents maintained in memory to a file on the switch. Configured through the **dhcp-snooping binding timeout** command.
Database Last Sync Time	The last date and time DHCP Snooping binding table entries were saved from memory to a file on the switch.
Binding Persistency Status	Indicates whether a binding table entry is retained (**Enabled**) or removed (**Disabled**) if the MAC address is missing from the MAC address table when the binding table database is synchronized. Configured through the **dhcp-snooping binding persistency** command.
DHCP Snooping Option-82 Policy	Indicates whether to **keep**, **replace**, or **drop** the Option-82 field information contained in DHCP packets received by the switch. Configured through the **dhcp-snooping option-82 policy** command.

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-snooping admin-state	Enables or disables DHCP Snooping for the switch.
dhcp-snooping vlan	Enables or disables DHCP Snooping at the VLAN level.

MIB Objects

```
dhcpSnoopingMode
dhcpSnoopingOpt82DataInsertionStatus
dhcpSnoopingMacAddrVerificationStatus
dhcpSnoopingBypassOpt82CheckStatus
dhcpSnoopingOption82FormatType
dhcpSnoopingOption82StringValue
dhcpSnoopingOption82Policy
dhcpSnoopingBindingStatus
dhcpSnoopingBindingDatabaseSyncTimeout
dhcpSnoopingBindingDatabaseLastSyncTime
dhcpSnoopingBindingPersistencyStatus
```

show dhcp-snooping ip-source-filter

Displays the ports or VLANs on which IP source filtering is enabled.

show dhcp-snooping ip-source-filter {vlan | port}

Syntax Definitions

vlan	Displays the VLANs on which IP source filtering is enabled.
port	Displays the ports on which IP source filtering is enabled.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The show output displays only those ports or VLANs on which IP source filtering is enabled.
- This command also displays the status of the link aggregate ports when source filtering is enabled at VLAN or port level.

Examples

```
-> show dhcp-snooping ip-source-filter port

Global Admin Status : Enabled

              IP Src
   Port      Filtering
----------+-------------
1/1/7       Enabled
1/1/12      Enabled
1/4/30      Enabled
1/4/35      Enabled
```

output definitions

Global Admin Status	The status of DHCP Snooping IP source filtering functionality for the switch (**Enabled** or **Disabled**).
Port	The chassis, slot, and port number.
IP Src Filtering	The IP source filtering status (**Enabled** or **Disabled**) for the port.

```
-> show dhcp-snooping ip-source-filter vlan

Global Admin Status : Enabled

 VLAN    Ip Src
  ID    Filtering
------+------------
 10     Enabled
 11     Enabled
```

output definitions

Global Admin Status	The status of DHCP Snooping IP source filtering functionality for the switch (**Enabled** or **Disabled**).
Vlan ID	The VLAN ID number.
IP Src Filtering	The IP source filtering status (**Enabled** or **Disabled**) for the VLAN ID.

Release History

Release 7.3.4; command introduced.
Release 8.6.R1; “Global Admin Status” field added.

Related Commands

dhcp-snooping ip-source-filter admin-state	Enables or disabled the DHCP Snooping IP source filtering functionality for the switch.
dhcp-snooping ip-source-filter	Enables or disables IP source filtering for a specific port, link aggregate, or VLAN.

MIB Objects

```
dhcpSnoopingIpSourceFilterAdminState
dhcpSnoopingSourceFilterVlanTable
   dhcpSnoopingSourceFilterVlanNumber
   dhcpSnoopingSourceFilterVlanFilteringStatus
dhcpSnoopingPortTable
   dhcpSnoopingPortIpSourceFiltering
```

show dhcp-snooping vlan

Displays a list of VLANs that have DHCP Snooping enabled and whether or not MAC address verification and Option-82 data insertion is enabled for each VLAN.

show dhcp-snooping vlan

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command only applies if DHCP Snooping is enabled at the VLAN level.
- Use the **show dhcp-snooping** command to determine the status of DHCP Snooping at the switch level.

Examples

```
-> show dhcp-snooping vlan
VLAN    Admin      Opt82        MAC Addr
 ID     State     Insertion   Verification
------+----------+----------+--------------
 50    Enabled    Enabled      Enabled
 60    Enabled    Enabled      Enabled
 100   Enabled    Disabled     Enabled
 200   Enabled    Enabled      Disabled
 300   Disabled   Enabled      Enabled
 1500  Disabled   Disabled     Disabled
```

output definitions

VLAN ID	The VLAN identification number for the DHCP Snooping VLAN.
Admin State	The administrative status of DHCP Snooping for the VLAN (**Enabled** or **Disabled**).
MAC Addr Verification	Indicates whether or not MAC address verification is enabled for the VLAN (**Enabled** or **Disabled**).
Opt-82 Insertion	Indicates whether or not Option-82 data insertion is enabled for the VLAN (**Enabled** or **Disabled**).

Release History

Release 7.3.4; command introduced.
Release 8.6R1; “Admin State” field added.

Related Commands

dhcp-snooping vlan	Enables or disables DHCP Snooping, MAC address verification, and Option-82 data insertion for the specified VLAN.
show dhcp-snooping	Displays the current DHCP Snooping configuration.
show dhcp-snooping port	Displays the trust mode and DHCP violation statistics for all switch ports that are filtered by DHCP Snooping.

MIB Objects

```
dhcpSnoopingVlanTable
   dhcpSnoopingVlanNumber
   dhcpSnoopingVlanMacAddrVerificationStatus
   dhcpSnoopingVlanOpt82DataInsertionStatus
   dhcpSnoopingVlanStatus
   dhcpSnoopingVlanAdminState
```

show dhcp-snooping port

Displays the trust mode and DHCP Snooping violation statistics for all switch ports and link aggregates that are filtered by DHCP Snooping.

show dhcp-snooping port

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If DHCP Snooping is operating at the switch level, then information for all switch ports and link aggregates is displayed.
- If DHCP Snooping is operating at the VLAN level, then information for only those ports and link aggregates that are associated with a DHCP Snooping VLAN is displayed.
- The violation statistics displayed only apply to ports and link aggregates that are in the client only trust mode. When the trust mode for a port is changed from **client-only** to **trusted** or **blocked**, the violation counters are set to zero (0).

Examples

```
-> show dhcp-snooping port
            Trust   Opt82       MAC       Server     Relay      Binding
   Port     Mode    Violation  Violation  Violation  Violation  Violation
----------+--------+----------+----------+----------+----------+----------
1/4/1      Blocked        0          0          0          0          0
1/4/2      Client         0          0          0          0          0
1/4/3      Client         0          0          0          0          0
1/4/4      Trusted        0          0          0          0          0
1/4/5      Client         0          0          0          0          0
 0/10      Trusted        0          0          0          0          0
```

output definitions

Port	The chassis, slot, and port number or a link aggregate ID number
Trust Mode	The DHCP Snooping trust mode for the port (**Blocked**, **Client**, or **Trusted**). Configured through the **dhcp-snooping port** command.
Opt82 Violation	The number of DHCP packets dropped due to a DHCP Snooping Option-82 violation.

output definitions (continued)

MAC Violation	The number of DHCP packets dropped due to a mismatch between the packet source MAC address and the client hardware address contained within the packet.
Server Violation	The number of DHCP server packets dropped because they originated from outside the network or firewall.
Relay Violation	The number of DHCP packets dropped because the packet included a relay agent IP address that was not 0.0.0.0.
Binding Violation	The number of DHCP packets dropped due to a mismatch between packets received and binding table information.

Release History

Release 7.3.4; command introduced.

Related Commands

show dhcp-snooping	Displays the current DHCP Snooping configuration.
show dhcp-snooping vlan	Displays a list of DHCP Snooping VLANs.
dhcp-snooping clear violation-counters	Clears the DHCP violation counters.

MIB Objects

```
dhcpSnoopingPortTable
   dhcpSnoopingPortIfIndex
   dhcpSnoopingPortTrustMode
   dhcpSnoopingPortOption82Violation
   dhcpSnoopingPortMacAddrViolation
   dhcpSnoopingPortDhcpServerViolation
   dhcpSnoopingPortRelayAgentViolation
   dhcpSnoopingPortBindingViolation
```

dhcp-snooping clear violation-counters

Clears the DHCP violation counters.

dhcp-snooping clear violation-counters {port *chassis/slot/port* **[-***port2***]} | slot** *chassis/slot* **| linkagg** *agg_id* **| all}**

Syntax Definitions

chassis/slot/port **[-***port2***]**	Clear DHCP snooping violation counters for the specified physical port or range of ports
chassis/slot	Clear DHCP snooping violation counters for all ports of the specified slot.
agg_id	Clear DHCP snooping violation counter for the specified link aggregate.
all	Clear DHCP snooping violation counters on all ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **port**, **slot**, or **linkagg** parameter options to clear the DHCP violation counters for a specific port, all ports on a chassis/slot, or a specific link aggregate.

Examples

```
-> dhcp-snooping clear violation-counters port 1/2
-> dhcp-snooping clear violation-counters port 1/2/3
-> dhcp-snooping clear violation-counters port 1/2/4-9
-> dhcp-snooping clear violation-counters linkagg 5
-> dhcp-snooping clear violation-counters slot 3/2
-> dhcp-snooping clear violation-counters all
```

Release History

Release 8.5R2; command introduced.

Related Commands

show dhcp-snooping port	Displays the trust mode and DHCP Snooping violation statistics for all switch ports that are filtered by DHCP Snooping.

MIB Objects

```
dhcpSnoopingClearViolationTable
   dhcpSnoopingClearViolationIfIndex
   dhcpSnoopingClearViolationAction
```

show dhcp-snooping counters

Displays the DHCP Snooping/Relay global counters.

show dhcp-snooping counters [slot *chassis_id/slot_id***]**

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

NI counters display the cumulative value from requested NIs.

Examples

```
-> show dhcp-snooping counters
DHCP Discover Packets                        : 226,
DHCP Offer Packets                           : 226,
DHCP Request Packets                         : 226,
DHCP ACK Packets                             : 226,
DHCP NACK Packets                            : 0,
DHCP Release Packets                         : 10,
DHCP Decline Packets                         : 0,
DHCP Inform Packets                          : 10,
DHCP Renew Packets                           : 0,
Total Packet received in CMM                 : 2,
Binding error (TCAM Unavailable)             : 0,
Unknown/Malformed Packets Dropped            : 0,
Packets received in CMM                      : 224,
Packets transmitted from CMM                 : 909,
Total ISF Packet Drop                        : 0

->show dhcp-snooping counters slot 1/1
Packet received in CMM from NI              : 472,
Packet transmitted from CMM to NI           : 453,
Packets received in NI from CMM             : 453,
Packets transmitted from NI to CMM          : 472,
Total ISF Packet Drop                       : 453,
```

output definitions

DHCP Discover Packets	Displays the number of Discover packets.
DHCP Offer Packets	Displays the number of Offer packets.
DHCP Request Packets	Displays the number of Request packets.

output definitions (continued)

DHCP ACK Packets	Displays the number Acknowledged packets.
DHCP NACK Packets	Displays the number of negative acknowledged packets.
DHCP Release Packets	Displays the number of Release packets.
DHCP Decline Packets	Displays the number of Decline packets.
DHCP Inform Packets	Displays the number of Inform packets.
DHCP Renew Packets	Displays the number of Renew packets,.
Total Packet received in CMM	Displays the total number of packets received in CMM.
Binding error (TCAM Unavailable)	Displays the number of Binding error.
Unknown/Malformed Packets Dropped	Displays the number of Unknown or Malformed packets dropped.
Packets received in CMM	Displays the number of packets received in CMM.
Packets transmitted from CMM	Displays the number of packets transmitted from CMM.
Total ISF Packet Drop	Displays the number of total ISF packets dropped.
Packets received in CMM from NI	Displays the number of packets received in CMM which is transmitted from NI.
Packets transmitted from CMM to NI	Displays the number of packets transmitted from CMM which is received in NI.
Packets received in NI from CMM	Displays the number of packets received in NI which is transmitted from CMM.
Packets transmitted from NI to CMM	Displays the number of packets transmitted from NI which is received in CMM.

Release History

Release 8.5R2; command introduced.

Related Commands

dhcp-snooping clear counters	Clears the global counters for DHCP Snooping/Relay.

MIB Objects

N/A

dhcp-snooping clear counters

Clears the global and per NI counters for DHCP Snooping/Relay.

dhcp-snooping clear counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When this command is used, the counter statistics displayed with the **show dhcp-snooping counters** command are reset to zero.

Examples

```
-> dhcp-snooping clear counters
```

Release History

Release 8.5R2; command introduced.

Related Commands

show dhcp-snooping counters	Displays the DHCP snooping/Relay global counters. NI counters display the cumulative value from requested NIs.

MIB Objects

N/A

show dhcp-snooping isf-statistics

Displays the IP source filter (ISF) drop counters.

show dhcp-snooping isf-statistics [vlan *vlan_id***]**

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **vlan** parameter to display counters for a specific VLAN ID.

Examples

```
-> show dhcp-snooping isf-statistics
Mode: Vlan based ISF
Chassis    Slot     Vlan     Packets Dropped
--------+--------+---------+-----------------
   1         1       10         300
   1         2       10         400
   1         3       11         500
   1         4       11         600

-> show dhcp-snooping isf-statistics vlan 10
Mode: Vlan based ISF
Chassis    Slot     Vlan     Packets Dropped
--------+--------+---------+-----------------
   1         1       10         300
   1         2       10         400

-> show dhcp-snooping isf-statistics
Mode: Port based ISF
Chassis    Slot     Vlan     Packets Dropped
--------+--------+---------+-----------------
   1         1       NA         300
   1         2       NA         400
   2         1       NA         500
   2         2       NA         600
```

Release History

Release 8.5R2; command introduced.

Related Commands

dhcp-snooping clear isf-statistics	Clears the ISF drop counters.

MIB Objects

N/A

dhcp-snooping clear isf-statistics

Clears the IP source filter (ISF) drop counters.

dhcp-snooping clear isf-statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When this command is used, the counter statistics displayed with the **show dhcp-snooping isf-statistics** command are reset to zero.

Examples

```
-> dhcp-snooping clear isf-statistics
```

Release History

Release 8.5R2; command introduced.

Related Commands

show dhcp-snooping isf-statistics	Displays the ISF drop counters.

MIB Objects

N/A

show dhcp-snooping binding

Displays the contents of the DHCP Snooping binding table (database).

show dhcp-snooping binding [port *chassis/slot/port***] | linkagg** *agg_id* **| ip-address** *ip_address* **| snapshot [static | dynamic]]**

Syntax Definitions

chassis/slot/port	The chassis, slot, and port number for which binding table entries are displayed.
agg_id	The link aggregate ID for which binding table entries are displayed.
ip_address	The IPv4 address.for which binding table entries are displayed.
snapshot	Displays binding table entries in the configuration snapshot format.
static	Displays only static binding table entries.
dynamic	Displays only dynamic binding table entries.

Defaults

By default, all binding table entries are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **dhcp-snooping binding** command to create a static entry in the binding table.
- Dynamic binding table entries are created when the relay agent receives a DHCPACK packet.

Examples

```
-> show dhcp-snooping binding

Total Number of Binding Entries: 12

       MAC                      IP          Lease    VLAN     Binding
     Address         Port      Address       Time      ID      Type
------------------+------+--------------+---------+-------+-----------
00:20:95:11:22:10   1/1/4  100.100.100.10     -        100    Static
02:00:00:00:0a:00   1/1/5  100.100.100.11    30        100    Dynamic
00:20:95:11:22:11   1/1/5  100.100.100.20     -        100    Static
02:00:00:00:02:00   1/1/6  100.100.100.10    30        100    Dynamic
02:00:00:00:09:00   1/1/6  100.100.100.18    30        100    Dynamic
02:00:00:00:08:00   1/1/6  100.100.100.6     30        100    Dynamic
02:00:00:00:05:00   1/1/6  100.100.100.8     30        100    Dynamic
02:00:00:00:03:00   1/1/7  100.100.100.3     30        100    Dynamic
02:00:00:00:01:00   1/1/7  100.100.100.17    30        100    Dynamic
02:00:00:00:07:00     0/1  100.100.100.13    30        100    Dynamic
02:00:00:00:04:00     0/1  100.100.100.15    30        100    Dynamic
00:20:95:11:22:12    0/10  100.100.100.30     -        100    Static
```

```
-> show dhcp-snooping binding port 1/1/5

Total Number of Binding Entries: 2

       MAC                        IP          Lease    VLAN     Binding
     Address         Port       Address       Time      ID      Type
------------------+------+--------------+---------+-------+-----------
02:00:00:00:0a:00   1/1/5  100.100.100.11    30        100    Dynamic
00:20:95:11:22:11   1/1/5  100.100.100.20     -        100    Static

-> show dhcp-snooping binding linkagg 1

Total Number of Binding Entries: 2

       MAC                        IP          Lease    VLAN     Binding
     Address         Port       Address       Time      ID      Type
------------------+------+--------------+---------+-------+-----------
02:00:00:00:07:00     0/1  100.100.100.13    30        100    Dynamic
02:00:00:00:04:00     0/1  100.100.100.15    30        100    Dynamic

-> show dhcp-snooping binding ip-address 100.100.100.11

Total Number of Binding Entries: 1

       MAC                        IP          Lease    VLAN     Binding
     Address         Port       Address       Time      ID      Type
------------------+------+--------------+---------+-------+-----------
02:00:00:00:0a:00   1/1/5  100.100.100.11    30        100    Dynamic

-> show dhcp-snooping binding snapshot static
dhcp-snooping binding 00:20:95:11:22:12 linkagg 10 address 100.100.100.30 vlan 100
dhcp-snooping binding 00:20:95:11:22:10 port 1/1/4  address 100.100.100.10 vlan 100
dhcp-snooping binding 00:20:95:11:22:11 port 1/1/5  address 100.100.100.20 vlan 100

-> show dhcp-snooping binding snapshot dynamic
dhcp-snooping binding 02:00:00:00:0a:00 port 1/1/5  address 100.100.100.11 vlan 100
dhcp-snooping binding 02:00:00:00:02:00 port 1/1/6  address 100.100.100.10 vlan 100
dhcp-snooping binding 02:00:00:00:09:00 port 1/1/6  address 100.100.100.18 vlan 100
dhcp-snooping binding 02:00:00:00:08:00 port 1/1/6  address 100.100.100.6 vlan 100
dhcp-snooping binding 02:00:00:00:05:00 port 1/1/6  address 100.100.100.8 vlan 100
dhcp-snooping binding 02:00:00:00:03:00 port 1/1/7  address 100.100.100.3 vlan 100
dhcp-snooping binding 02:00:00:00:01:00 port 1/1/7  address 100.100.100.17 vlan 100
dhcp-snooping binding 02:00:00:00:07:00 linkagg 1  address 100.100.100.13 vlan 100
dhcp-snooping binding 02:00:00:00:04:00 linkagg 1  address 100.100.100.15 vlan 100
```

output definitions

MAC Address	The MAC address of the client.
Port	The chassis/slot/port designation for the switch port that received the DHCP request.
IP Address	The IP address offered by the DHCP server.
Lease Time	The IP address lease time assigned by the DHCP server. A value of 0 indicates a static entry.
VLAN ID	The VLAN ID of the VLAN to which the client belongs.
Binding Type	Indicates whether the binding table entry is **dynamic** or **static**. Static entries are created using the **dhcp-snooping binding** command.

Release History

Release 7.3.4; command introduced.
Release 8.5R2; **snapshot, static, dynamic** parameters added.
Release 8.6R1; **port**, **linkagg**, **ip-address** parameters added.

Related Commands

show dhcp-snooping	Displays the current DHCP Snooping configuration.
show dhcp-snooping vlan	Displays a list of DHCP Snooping VLANs.
show dhcp-snooping port	Displays the trust mode and DHCP violation statistics for all switch ports that are filtered by DHCP Snooping.

MIB Objects

```
dhcpSnoopingBindingStatus
dhcpSnoopingBindingTable
   dhcpSnoopingBindingMacAddress
   dhcpSnoopingBindingIfIndex
   dhcpSnoopingBindingIpAddress
   dhcpSnoopingBindingLeaseTime
   dhcpSnoopingBindingVlan
   dhcpSnoopingBindingType
```

dhcpv6-snooping vlan admin-state

Enables or disables DHCPv6 Snooping on a per-VLAN basis.

dhcpv6-snooping vlan *vlan_id***[-***vlan_id2***] admin-state {enable | disable}**

no dhcpv6-snooping vlan *vlan_id***[-***vlan_id2***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	The VLAN ID on which DHCPv6 Snooping must be enabled or disabled. Use a hyphen to specify a range of VLANs (10-15).
enable	Enables DHCPv6 Snooping on the specified VLAN.
disable	Disables DHCPv6 Snooping on the specified VLAN.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- DHCPv6 Snooping can be enabled on per-VLAN basis or globally on the switch.
- The global DHCPv6 Snooping must be disabled before enabling the per-VLAN DHCPv6 Snooping.
- When DHCPv6 Snooping is configured on a per-VLAN basis, DHCPv6 snooping is limited to a maximum of 64 VLANs.
- DHCPv6 snooping must not be enabled in configurations where a DHCPv6 server assigns multiple addresses to a client. In such situations, only the first address will be stored in the binding table.
- To completely remove DHCPv6 snooping configuration from a VLAN, use the **no** form of the command.

Examples

```
-> dhcpv6-snooping vlan 1 admin-state enable
-> dhcpv6-snooping vlan 10-20 admin-state enable
-> dhcpv6-snooping vlan 1 admin-state disable
-> dhcpv6-snooping vlan 10-20 admin-state disable
-> no dhcpv6-snooping vlan 2
-> no dhcpv6-snooping vlan 10-20
```

Release History

Release 8.5R3; command introduced.
Release 8.6R2; VLAN range added.

Related Commands

dhcpv6-snooping binding	Configures a static entry in the binding table.
dhcpv6-snooping binding persistency	Configures whether to retain or not retain the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.
dhcpv6-snooping ipv6-source-filter	Enables or disables the IPv6 source filtering capability at a port, link aggregation, or VLAN level using the DHCPv6 Snooping binding table.
show dhcpv6-snooping	Displays the global DHCPv6 Snooping configuration.
show dhcpv6-snooping interfaces	Displays the DHCPv6 Snooping configuration status on per-VLAN.

MIB Objects

```
alaiDHCPv6SnoopingTable
   alaDHCPv6SnoopingInterfaceIndex
   alaDHCPv6SnoopingInterfaceAdminStatus
   alaDHCPv6SnoopingInterfaceRowStatus
```

dhcpv6-snooping global admin-state

Enables or disables DHCPv6 Snooping globally on the switch.

dhcpv6-snooping global admin-state {enable | disable}

Syntax Definitions

global	The DHCPv6 Snooping is enabled or disabled globally on the switch.
enable	Enables DHCPv6 Snooping for the switch.
disable	Disables DHCPv6 Snooping for the switch.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- DHCPv6 Snooping can be enabled on per-VLAN or globally on the switch.
- The per-VLAN DHCPv6 Snooping must be disabled before enabling global DHCPv6 Snooping.
- DHCPv6 snooping must not be enabled in configurations where a DHCPv6 server assigns multiple addresses to a client. In such situations only the first address will be stored in the binding table.

Examples

```
-> dhcpv6-snooping global admin-state enable
-> dhcpv6-snooping global admin-state disable
```

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping binding	Configures a static entry in the binding table.
dhcpv6-snooping binding persistency	Allows to configure whether to retain or not retain the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.
dhcpv6-snooping ipv6-source-filter	Enables or disables the IPv6 source filtering capability at a port, link aggregation, or VLAN level using the DHCPv6 Snooping binding table.
show dhcpv6-snooping	Displays the global DHCPv6 Snooping configuration.
show dhcpv6-snooping interfaces	Displays the DHCPv6 Snooping configuration status on per-VLAN.

MIB Objects

```
alaiDHCPv6SnoopingTable
   alaDHCPv6SnoopingInterfaceIndex
   alaDHCPv6SnoopingInterfaceAdminStatus
   alaDHCPv6SnoopingInterfaceRowStatus
```

dhcpv6-snooping binding

Configures a static entry in the binding table.

dhcpv6-snooping binding vlan *vlan_id* **link-local** *ipv6_address* **[global-address** *ipv6_address***] [mac-address** *mac_address***] [port** *chassis/slot/port* **| linkagg** *agg_id***]**

no dhcpv6-snooping binding vlan *vlan_id* **link-local** *ipv6_address*

Syntax Definitions

vlan_id	The VLAN ID on which the DHCPv6 client is configured.
link-local	The clients link-local IPV6 address.
global-address	The IPV6 global unicast address assigned by the DHCPv6 lease server.
mac-address	The clients MAC address.
port | linkagg	The port or link aggregate used to reach the DHCPv6 client.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- When a new binding entry is added or an existing entry is modified using this command, the entry's lease lifetime is changed to indefinite.
- While adding a new binding entry the values for all the parameters must be specified. Else, the binding entry will not be added.
- When a VLAN is deleted, all binding entries on the VLAN including the manually added binding entry is also removed.

Examples

```
-> dhcpv6-snooping binding vlan 1 link-local fe80::eae7:32ff:fea4:6321 global-
address 2001:db8:1000::2b0:d0ff:fe86:880e mac-address 00:00:01:1d:4f:7d linkagg 1
-> no dhcpv6-snooping binding vlan 1 link-local fe80::eae7:32ff:fea4:6321
```

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping global admin-state	Enables or disables DHCPv6 Snooping globally on the switch.
dhcpv6-snooping vlan admin-state	Enables or disables DHCPv6 Snooping on a per-VLAN basis.
show dhcpv6-snooping binding	Displays the DHCPv6 Snooping binding table information.

MIB Objects

```
alaiDHCPv6BindingTable
   alaDHCPv6SnoopingInterfaceIndex
   alaDHCPv6BindingLinkLocalAddress
   alaDHCPv6BindingGlobalAddress
   alaDHCPv6BindingPhysAddress
   alaDHCPv6BindingPortIfIndex
```

dhcpv6-snooping binding timeout

Configures the amount of time between each automatic save of the DHCPv6 Snooping binding table contents maintained in memory to a file on the switch.

dhcpv6-snooping binding timeout *seconds*

Syntax Definitions

seconds	The time interval in seconds between automatic save of the DHCPv6 Snooping binding table to file on the switch. The time interval range is 1 to 600 seconds.

Defaults

The default value is 1 second.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

The timeout value is only valid if the DHCPv6 Snooping binding table functionality is enabled.

Examples

```
-> dhcpv6-snooping binding timeout 5
```

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping binding	Configures a static entry in the binding table.
show dhcpv6-snooping binding	Displays the DHCPv6 Snooping binding table information.

MIB Objects

```
alaDHCPV6BindingConfig
   alaDHCPv6BindingTimeout
```

dhcpv6-snooping binding action

Allows to manually purge, renew or save the DHCPv6 Snooping binding table.

dhcpv6-snooping binding action {purge | renew | save}

Syntax Definitions

purge	Clears the content of the DHCPv6 binding table.
renew	Restores the DHCPv6 binding table entries with the previously saved values in the permanent storage.
save	Saves the DHCPv6 binding table entries to permanent storage.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- The DHCPv6 Snooping binding table is maintained in the switch memory. Binding table entries are saved on a periodic basis to the file on the switch. Use the purge, renew, and save options available with this command to sync the binding table contents with the contents of the file.
- While using binding table action commands ensure the binding timeout interval is set greater than 10 seconds from the default interval 1 second to avoid quick timeout.

Examples

```
-> dhcpv6-snooping binding action purge
-> dhcpv6-snooping binding action renew
-> dhcpv6-snooping binding action save
```

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping binding	Configures a static entry in the binding table.
show dhcpv6-snooping binding	Displays the DHCPv6 Snooping binding table information.

MIB Objects

```
alaDHCPV6BindingConfig
   alaDHCPv6BindingAction
```

dhcpv6-snooping binding persistency

Configures whether to retain or not retain the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.

dhcpv6-snooping binding persistency {enable | disable}

Syntax Definitions

enable	Enables DHCPv6 Snooping binding persistency. The DHCPv6 Snooping binding table entries will be retained even if the MAC address is deleted from the switch's MAC cache.
disable	Disables DHCPv6 Snooping binding persistency. The DHCPv6 Snooping binding table entries will be deleted if the MAC address is deleted from the switch's MAC cache.

Defaults

By default, DHCPv6 snooping binding persistency is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- If the binding table is restored from permanent storage when the DHCPv6 Snooping binding persistency is enabled, all entries will be added to the binding table, even if the MAC address is not in the switch's MAC cache.
- If the binding table is restored from permanent storage when the DHCPv6 Snooping binding persistency is disabled, only entries for which there is a corresponding entry in the switch's MAC cache will be restored.
- The binding entries will get deleted upon lease time expiry and also during link down or MAC address deletion unless persistency is enabled on the switch.

Examples

```
-> dhcpv6-snooping binding persistency enable
-> dhcpv6-snooping binding persistency disable
```

Release History

Release 8.5R3; command introduced.

Related Commands

show dhcpv6-snooping binding Displays the DHCPv6 Snooping binding table information.

MIB Objects

```
alaDHCPV6BindingConfig
   alaDHCPv6BindingPersistency
```

dhcpv6-snooping ipv6-source-filter

Enables or disables the IPv6 source filtering capability for a port, link aggregate, or VLAN using the DHCPv6 Snooping binding table.

dhcpv6-snooping ipv6-source-filter {vlan *vlan_id***[-***vlan_id2***] | port** *chassis/slot1/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} admin-state {enable | disable}**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	The VLAN ID on which the IPv6 source filtering needs to be enabled or disabled. Use a hyphen to specify a range of VLAN IDs (10-15).
*chassis/slot1/port***[-***port2***]**	The port number on which the IPv6 source filtering needs to be enabled or disabled. Use a hyphen to specify a range of ports (1/1/3-8).
*agg_id***[-***agg_id2***]**	The linkagg ID on which the IPv6 source filtering needs to be enabled or disabled. Use a hyphen to specify a range of IDs (1-5).
enable	Enables IPv6 source filtering for the specified port, link aggregation, or VLAN.
disable	Disables IPv6 source filtering for the specified port, link aggregation, or VLAN level.

Defaults

By default, IPv6 source filtering is disabled on port, link aggregation, or VLAN level.

Platforms Supported

OmniSwitch 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- DHCPv6 Snooping must be enabled for IPv6 source filtering to be enabled.
- IPv6 source filtering can be enabled per-VLAN or per-port (linkagg).
- If DHCPv6 Snooping is enabled on switch level, then IPv6 source filtering can be enabled on any port, linkagg or VLAN.
- If DHCPv6 Snooping is enabled on VLAN, then IPv6 source filtering can only be enabled on ports which are part of that VLAN, or on the same VLAN.
- If a static host is connected to IPv6 source filtering enabled port or VLAN, then all the packets coming from this host are dropped. A static binding entry must be created to allow the packets coming from this host to pass.
- To support IPv6 source filtering on an OmniSwitch 6560, use the **capability profile tcam mode** command to set the TCAM mode to source IPv6 filtering. After the TCAM mode is changed, reboot the switch to activate the source IPv6 filtering mode.

Examples

```
-> dhcpv6-snooping ipv6-source-filter vlan 1 admin-state enable
-> dhcpv6-snooping ipv6-source-filter vlan 10-15 admin-state enable
-> dhcpv6-snooping ipv6-source-filter port 1/1/2 admin-state enable
-> dhcpv6-snooping ipv6-source-filter port 1/1/3-8 admin-state enable
-> dhcpv6-snooping ipv6-source-filter linkagg 6 admin-state enable
-> dhcpv6-snooping ipv6-source-filter linkagg 1-5 admin-state enable

-> dhcpv6-snooping ipv6-source-filter vlan 1 admin-state disable
-> dhcpv6-snooping ipv6-source-filter vlan 10-15 admin-state disable
-> dhcpv6-snooping ipv6-source-filter port 1/1/2 admin-state disable
-> dhcpv6-snooping ipv6-source-filter port 1/1/3-8 admin-state disable
-> dhcpv6-snooping ipv6-source-filter linkagg 6 admin-state disable
-> dhcpv6-snooping ipv6-source-filter linkagg 1-5 admin-state disable
```

Release History

Release 8.5R3; command introduced.
Release 8.6R2; VLAN, port, and link aggregate range added.

Related Commands

dhcpv6-snooping vlan admin-state	Enables or disables DHCPv6 Snooping on a per-VLAN basis.
dhcpv6-snooping global admin-state	Enables or disables DHCPv6 Snooping globally on the switch.
show dhcpv6-snooping ipv6-source-filter	Displays the port, VLAN or link aggregation on which IPv6 Source Filter (ISF) is configured.

MIB Objects

```
alaDHCPV6SourceFilterInterfaceTable
   alaDHCPv6SourceFilterVlanId
   alaDHCPv6SourceFilterInterfaceIfIndex
   alaDHCPv6SourceFilterInterfaceRowStatus
   alaDHCPv6SourceFilterVlanRowStatus
```

ipv6 dhcp guard

Enables or disables DHCPv6 Guard on a VLAN. If enabled (the default), DHCPv6 server messages are discarded unless the messages are received on trusted ports. This command also includes an option to enable DHCPv6 Guard for client messages.

ipv6 dhcp guard vlan *vlan_id* **[client {enable | disable}] [admin-state {enable | disable}]**

no ipv6 dhcp guard vlan *vlan_id*

Syntax Definitions

vlan_id	The VLAN ID on which the DHCPv6 Guard is configured.
client enable	Enables DHCPv6 Guard for client messages. Multicast client-originated messages are sent out only on trusted ports. If there are no configured trusted ports, the client messages are dropped.
client disable	Disables DHCPv6 Guard for client messages. Client-originated messages are not checked.
admin-state enable	Enables DHCPv6 guard for server messages. DHCPv6 server messages that are not received on configured trusted ports are dropped. Enabling DHCPv6 Guard helps to prevent access from rogue DHCPv6 servers.
admin-state disable	Disables DHCPv6 Guard. Server messages are not checked.

Defaults

parameter	default
client enable | disable	disable
admin-state enable | disable	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- Trusted source ports serve as a filtering mechanism and are identified using the **ipv6 dhcp guard trusted** command.
  - Only DHCPv6 server messages received on trusted ports are allowed.
  - Client multicast messages are sent out only on trusted ports rather than flooded out on all ports in the VLAN.
- Enabling DHCPv6 Guard without configuring any trusted ports helps to prevent unwanted DHCPv6 traffic flow. For example:
  - DHCPv6 server messages are discarded, which helps to prevent messages from reaching clients on the VLAN.
  - If the client option is also enabled, then DHCPv6 multicast client messages are also discarded. This helps to prevent DHCPv6 traffic from getting past the switch. If there are no client messages sent out, then there are no responses sent from the DHCPv6 server.

- Use the **no** form of this command to remove the DHCPv6 Guard configuration, which includes removing any configured trusted ports for the VLAN.

Examples

```
-> ipv6 dhcp guard vlan 200 admin-state enable
-> ipv6 dhcp guard vlan 200 admin-state disable
-> ipv6 dhcp guard vlan 200 client enable
-> ipv6 dhcp guard vlan 200 client disable
-> no ipv6 dhcp guard vlan 200
```

Release History

Release 8.5R2; command introduced.
Release 8.6R1; **vlan** and **client** parameters added, *if_name* parameter deprecated.

Related Commands

ipv6 dhcp guard trusted	Configures the DHCPv6 Guard trusted source ports.
show ipv6 dhcp guard	Displays the DHCPv6 Guard configuration.

MIB Objects

```
alaDHCPv6GuardInterfaceTable
   alaDHCPv6GuardInterfaceEntry
   alaDHCPv6GuardInterfaceAdminStatus
   alaDHCPv6GuardInterfaceClient
   alaDHCPv6GuardInterfaceRowStatus
```

ipv6 dhcp guard trusted

Configures the DHCPv6 Guard trusted source ports.

ipv6 dhcp guard vlan *vlan_id* **trusted [port** *chassis/slot/port* **| linkagg** *agg_id***]**

no ipv6 dhcp guard vlan *vlan_id* **trusted [port** *chassis/slot/port* **| linkagg** *agg_id***]**

Syntax Definitions

vlan_id	The VLAN ID on which DHCPv6 Guard is configured.
chassis/slot/port	The *chassis/slot/port* on which the DHCPv6 server messages must be allowed. Make sure the port is a member of the specified VLAN.
agg_id	The link aggregate ID on which the DHCPv6 server messages must be allowed. Make sure the link aggregate ID is a member of the specified VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- When DHCPv6 Guard is enabled, trusted source ports serve as a filtering mechanism.
  - Only DHCPv6 server messages received on trusted ports are allowed. This functionality helps to prevent access from rogue DHCPv6 servers.
  - Client multicast messages are sent out only on trusted ports rather than flooded out on all ports in the VLAN.
- Enabling DHCPv6 Guard without configuring any trusted ports helps to prevent unwanted DHCPv6 traffic flow. For example:
  - DHCPv6 server messages are discarded, which helps to prevent messages from reaching clients on the VLAN.
  - DHCPv6 multicast client messages are also discarded, which helps to prevent DHCPv6 traffic from getting past the switch. If there are no client messages sent out, then there are no responses sent from the DHCPv6 server.
- Use the **no** form of the command to remove the DHCPv6 Guard trusted source.

Examples

```
-> ipv6 dhcp guard vlan 200 trusted port 2/1/11
-> ipv6 dhcp guard vlan 200 trusted linkagg 10
-> no ipv6 dhcp guard vlan 200 trusted port 2/1/11
```

Release History

Release 8.5R2; command introduced.
Release 8.6R1; **vlan** parameter added, *if_name* parameter deprecated.

Related Commands

ipv6 dhcp guard	Enables or disables the DHCPv6 Guard on a VLAN.
show ipv6 dhcp guard	Displays the DHCPv6 Guard configuration.

MIB Objects

```
alaDHCPv6GuardTrustedSourceTable
   alaDHCPv6GuardTrustedSourceIfIndex
   alaDHCPv6GuardTrustedSourceRowStatus
```

show dhcpv6-snooping

Displays the global DHCPv6 Snooping configuration.

show dhcpv6-snooping

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show dhcpv6-snooping
DHCPv6 Snooping       = Global,
Binding timeout (sec) = 1,
Binding persistency   = Disabled
```

output definitions

DHCPv6 Snooping	Displays if the DHCPv6 Snooping is enabled globally or Per-VLAN mode.
Binding timeout	Displays the binding table automatic save timeout.
Binding persistency	Displays the configured DHCPv6 Relay destination(s) for the interface.

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping vlan admin-state	Enables or disables DHCPv6 Snooping on a per-VLAN basis.
dhcpv6-snooping global admin-state	Enables or disables DHCPv6 Snooping globally on the switch.
dhcpv6-snooping binding timeout	Configures the amount of time between each automatic save of the DHCPv6 Snooping binding table contents maintained in memory to a file on the switch.
dhcpv6-snooping binding persistency	Configures whether to retain or not retain the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.

MIB Objects

```
alaDHCPv6SnoopingInterfaceAdminStatus
alaDHCPv6BindingTimeout
alaDHCPv6BindingPersistency
```

show dhcpv6-snooping interfaces

Displays the DHCPv6 Snooping configuration status per-VLAN.

show dhcpv6-snooping interfaces

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show dhcpv6-snooping interfaces
Interface                 Admin Status
--------------------------+----------------
VLAN 11                   Enabled
VLAN 99                   Disabled
```

output definitions

Interface	Displays the VLAN on which DHCPv6 Snooping is configured.
Admin Status	Displays the operational status of DHCPv6 Snooping on the VLAN interface.

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping vlan admin-state	Enables or disables DHCPv6 Snooping on a per-VLAN basis.
dhcpv6-snooping global admin-state	Enables or disables DHCPv6 Snooping globally on the switch.

MIB Objects

```
alaDHCPv6SnoopingInterfaceIndex
alaDHCPv6SnoopingInterfaceAdminStatus
```

show dhcpv6-snooping binding

Displays the DHCPv6 Snooping binding table information.

show dhcpv6-snooping binding [global-address *ipv6_address***] [port** *chassis/slot/port* **| linkagg** *agg_id***]**

Syntax Definitions

ipv6_address	The IPV6 global unicast address for which binding table entries are displayed.
chassis/slot/port	The chassis, slot, and port number for which binding table entries are displayed.
agg_id	The link aggregate ID for which binding table entries are displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show dhcpv6-snooping binding
Total Number of Binding Entries: 3
Link-Local Address         Global Address  Lifetime   Interface  Port   MAC Address
--------------------------+--------------+----------+----------+------+-----------------
fe80::02aa:81ff:febb:0101  2001:db8:11::1  2000       VLAN 11    1/1/1  00:AA:81:BB:01:01
fe80::02aa:81ff:febb:0202  2001:db8:11::2  indefinite VLAN 11    1/1/2  00:AA:81:BB:02:02
fe80::02cc:99ff:fe11:3131  2001:db8:99::33 static     VLAN 99    agg 7  00:CC:99:11:31:31

-> show dhcpv6-snooping binding port 1/1/1
Total Number of Binding Entries: 1
fe80::02aa:81ff:febb:0101  2001:db8:11::1  2000       VLAN 11    1/1/1  00:AA:81:BB:01:01

-> show dhcpv6-snooping binding global-address 2001:db8:11::2
Total Number of Binding Entries: 1
Link-Local Address         Global Address  Lifetime   Interface  Port   MAC Address
--------------------------+--------------+----------+----------+------+-----------------
fe80::02aa:81ff:febb:0202  2001:db8:11::2  indefinite VLAN 11    1/1/2  00:AA:81:BB:02:02

-> show dhcpv6-snooping binding linkagg 7
Total Number of Binding Entries: 1
Link-Local Address         Global Address  Lifetime   Interface  Port   MAC Address
--------------------------+--------------+----------+----------+------+-----------------
sfe80::02cc:99ff:fe11:3131  2001:db8:99::33 static     VLAN 99    agg 7  00:CC:99:11:31:31
```

output definitions

Total Number of Binding Entries	The total number of binding entries in the switch.
Link-Local Address	The link-local address of the client.
Global Address	The global IPv6 address obtained through the DHCPv6 lease.
Lifetime	The lifetime of the DHCPv6 lease. The lifetime is displayed in seconds. The lifetime is displayed as **indefinite** for the leases with indefinite lifetime. The lifetime is displayed as **static** if the time is manually configured.
Interface	The VLAN on which the client exists.
Port	The physical port or link aggregation used to communicate with the client.
MAC Address	The MAC address of the client.

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping binding	Configures a static entry in the binding table.
dhcpv6-snooping binding timeout	Allows to configure the amount of time between each automatic save of the DHCPv6 Snooping binding table contents maintained in memory to a file on the switch.
dhcpv6-snooping binding action	Allows to manually purge, renew or save the DHCPv6 Snooping binding table.

MIB Objects

```
alaDHCPv6BindingLinkLocalAddress
alaDHCPv6BindingPortIfIndex
alaDHCPv6BindingLeasedAddress
alaDHCPv6BindingLeaseTime
alaDHCPv6BindingType
alaDHCPv6SnoopingInterfaceIndex
alaDHCPv6BindingPhysAddress
```

show dhcpv6-snooping ipv6-source-filter

Displays the port, VLAN or link aggregation on which IPv6 Source Filter (ISF) is configured.

show dhcpv6-snooping ipv6-source-filter

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show dhcpv6-snooping ipv6-source-filter

Mode: Vlan based ISF

VLAN ID
---------------
  10-15
  20

-> show dhcpv6-snooping ipv6-source-filter

Mode: Port based ISF

PORT
---------------
 1/1/10
 1/1/15-20
 0/2
```

output definitions

VLAN ID	Displays the VLAN on which the ISF is enabled.
PORT	Displays the port or link aggregation on which the ISF is enabled.

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping ipv6-source-filter	Enables or disables the IPv6 source filtering capability at a port, link aggregation, or VLAN level using the DHCPv6 Snooping binding table.

MIB Objects

```
alaDHCPv6SourceFilterVlanId
alaDHCPv6SourceFilterInterfaceIfIndex
```

show ipv6 dhcp guard

Displays the DHCPv6 Guard configuration.

show ipv6 dhcp guard [vlan *vlan_id***]**

Syntax Definitions

vlan_id	Displays the DHCPv6 Guard configuration for the specified VLAN.

Defaults

By default, a summary table of information about all VLANs on which DHCPv6 Guard is configured is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

Specify the **vlan** *vlan_id* option to view the DHCPv6 Guard configuration for a specific VLAN.

Examples

```
-> show ipv6 dhcp guard
Interface                       Status   Client   Trusted Ports
--------------------------------+--------+--------+--------------------------------
VLAN 200                        Enabled  Disabled 1/1/9, 1/1/10, 1/1/11, 1/1/12+
VLAN 250                        Enabled  Disabled
VLAN 300                        Enabled  Enabled  agg 10, 1/4/20
```

output definitions

Interface	Displays the VLAN on which the DHCPv6 Guard is configured.
Status	Displays the status of DHCPv6 Guard (**Enabled** or **Disabled**).
Client	Displays the status of DHCPv6 Guard for client messages (**Enabled** or **Disabled**).
Trusted Ports	Displays the DHCPv6 Guard trusted sources. A '+' will appear at the end of the list to indicate that there are more trusted sources configured which cannot be displayed in a single line. To view the full list of configured trusted sources, specify the VLAN ID in the show command.

```
-> show ipv6 dhcp guard vlan 200
DHCPv6 Guard = Enabled
Client Guard = Disabled
Trusted ports:
  1/1/9
  1/1/10
  1/1/11
  1/1/12
  1/1/20
```

```
-> show ipv6 dhcp guard vlan 250
DHCPv6 Guard = Enabled
Client Guard = Disabled

-> show ipv6 dhcp guard vlan 300
DHCPv6 Guard = Enabled
Client Guard = Enabled
Trusted ports:
  linkagg 10
  1/4/20
```

output definitions

DHCPv6 Guard	Displays the status of DHCPv6 Guard on the VLAN.
Client Guard	Displays the status of DHCPv6 Guard for client messages.
Trusted ports	Displays the DHCPv6 Guard trusted sources, if any. Ports are displayed as *chassis/slot/port*. Link aggregates are displayed as linkagg ID.

Release History

Release 8.5R2; command introduced.
Release 8.561; **vlan** parameter added.

Related Commands

ipv6 dhcp guard	Enables or disables the DHCPv6 Guard on a VLAN.
ipv6 dhcp guard trusted	Configures DHCPv6 Guard trusted source ports.

MIB Objects

```
alaDHCPv6GuardInterfaceTable
   AlaDHCPv6GuardInterfaceEntry
   alaDHCPv6GuardInterfaceAdminStatus
   alaDHCPv6GuardInterfaceClient
alaDHCPv6GuardTrustedSourceTable
   alaDHCPv6GuardTrustedSourceIfIndex
```

25 VRRP Commands

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure in a default route environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the IPv4 or IPv6 VRRP routers on the LAN. The VRRP router that controls the IPv4 or IPv6 address associated with a virtual router is called the master router and is responsible for forwarding packets to that IPv4 or IPv6 address. If the master router becomes unavailable, the highest priority backup router will transition to the master state. The OmniSwitch implementation of VRRP also supports the collective management of virtual routers on a switch.

The VRRP commands comply with RFC 3768 for VRRP version 2 (IPv4) and RFC 5798 for VRRP version 3 (IPv4 and IPv6).

MIB information is as follows:

Filename: VRRP-MIB.mib
Module: vrrpMIB

Filename: VRRPV3-MIB.mib
Module: vrrpv3MIB

Filename: ALCATEL-IND1-VRRP-MIB.mib
Module: alcatelIND1VRRPMIB

Filename: ALCATEL-IND1-VRRP3-MIB.mib
Module: alcatelIND1VRRP3MIB

A summary of the available VRRP commands is listed here:

vrrp

Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.

{ip | ipv6} vrrp *vrid* **interface** *if_name* **admin-state [enable | disable] [priority** *priority***] [preempt | no preempt] [accept | no accept] [interval** *centiseconds***] [version {v2 | v3}**

no {ip | ipv6} *vrid* **interface** *if_name*

Syntax Definitions

ip	Configures an IPv4 virtual router.
ipv6	Configures an IPv6 virtual router.
vrid	The virtual router ID. The valid range is 1–255.
if_name	The name of an existing IPv4 or IPv6 interface on which the virtual router is configured.
enable	Enables the virtual router. An IPv4 virtual router may only be enabled if an IP address is configured for the virtual router (not required to enable an IPv6 virtual router).
disable	Disables the virtual router. Cannot be combined on the same line with other parameters.
priority	The priority for this virtual router to become the master router. The range is 1 (lowest priority) to 255 (highest priority). The priority should be set to 255 only if this router is the actual owner of the virtual router's IP address.
preempt	Specifies that a higher priority router may preempt a lower priority master router. However, the virtual router's actual IP address owner will always preempt another master router regardless of whether preempt is enabled.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router.
accept	Specifies that the master router, which is not the IP address owner, will accept the packets addressed to the IP address owner as its own. *This parameter applies only to IPv4 version 3 and IPv6 virtual routers.*
no accept	Specifies that the master router, which is not the IP address owner, will not accept the packets addressed to the IP address owner as its own. *This parameter applies only to IPv4 version 3 and IPv6 virtual routers.*
centiseconds	The interval in centiseconds after which the master router will send VRRP advertisements. The advertising interval must be the same for all VRRP routers configured with the same VRID. The range is 1–4095 centiseconds in increments of 10 (for example, 10, 20, 30).
v2	Converts an IPv4 VRRP router to a version 2 virtual router. *This parameter applies only to IPv4 virtual routers; IPv6 virtual routers are always version 3.*

v3	Converts an IPv4 VRRP router to a version 3 virtual router. *This parameter applies only to IPv4 virtual routers; IPv6 virtual routers are always version 3.*

Defaults

parameter	default
enable | disable	**disable**
priority	100
preempt | no preempt	**preempt**
accept | no accept	**accept**
centiseconds	100
v2 | v3	**v2**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a virtual router from the configuration.
- Use the **ip vrrp address** command to configure an IPv4 address for the virtual router. This must be done before the IPv4 virtual router can be enabled (not required to enable an IPv6 virtual router).
- To disable the virtual router, rather than remove it, use the **admin-state disable** option. Note that this option cannot be used with any other optional parameter.
- A virtual router must be disabled before it can be modified.
- A priority value of 255 indicates that the VRRP router owns the IP address; that is, the router contains the real physical interface to which the IP address is assigned. The system automatically sets this value to 255 if it detects that this router is the IP address owner. If the priority is set to 255 and the virtual router is not the IP address owner, then the priority will be set to the default value of 100. The IP address owner will always be the master router if it is available.
- VRRP routers backing up a virtual router must use priority values from 1 to 255. The default priority value for VRRP routers backing up a virtual router is 100. If you configure more than one backup, their priority values should be different. The **preempt** or **no preempt** setting specifies whether or not a higher priority router may preempt a lower priority master router.
- The maximum number of virtual routers supported is based on the 100 centisecond advertising interval. A smaller interval will result in a relatively lesser number of virtual routers.
- The advertising interval for IPv4 and IPv6 virtual routers
- The advertising interval for IPv4 and IPv6 virtual routers cannot be less than 10 centiseconds and must increment by 10 (for example, 10, 20, 30) up to the maximum allowed.

Examples

```
-> ip vrrp 23 interface ipv4-100 priority 75
-> ip vrrp 23 interface ipv4-100 address 192.168.173.1
-> ip vrrp 23 interface ipv4-100 admin-state enable

-> ip vrrp 23 interface ipv4-100 admin-state disable
-> ip vrrp 23 interface ipv4-100 priority 255
-> ip vrrp 23 interface ipv4-100 admin-state enable

-> no ip vrrp 23 interface ipv4-100

-> ipv6 vrrp 33 interface ipv6-200 priority 75
-> ipv6 vrrp 33 interface ipv6-200 admin-state enable

-> ipv6 vrrp 33 interface ipv6-200 admin-state disable
-> ipv6 vrrp 33 interface ipv6-200 priority 50
-> ipv6 vrrp 33 interface ipv6-200 admin-state enable

-> no ipv6 vrrp 33 interface ipv6-200
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; **interface** and **version** parameter added; *vlan_id* parameter deprecated.

Related Commands

vrrp address	Configures an IPv4 or an IPv6 address for a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
vrrpv3OperationsTable
   vrrpv3OperationsPriority
   vrrpv3OperationsPreemptMode
   vrrpv3OperationsAcceptMode
   vrrpv3OperationsAdvInterval
   vrrpv3OperationsRowStatus
alaVrrpv3OperationsExTable
   alaVrrpv3OperVersion
```

vrrp address

Configures an IPv4 or IPv6 address for a VRRP virtual router.

{ip | ipv6} vrrp *vrid* **interface** *if_name* **address {***ipv4_address* **|** *ipv6_address***}**

{ip | ipv6} vrrp *vrid* **interface** *if_name* **no address {***ipv4_address* **|** *ipv6_address***}**

Syntax Definitions

ip	Configures an IPv4 address for a virtual router.
ipv6	Configures an IPv6 address for a virtual router.
vrid	The virtual router ID. The valid range is 1–255.
if_name	The name of an existing IPv4 or IPv6 interface on which the virtual router is configured.
ipv4_address	The virtual IPv4 address to associate with the specified virtual router.
ipv6_address	The virtual IPv6 address to associate with the specified virtual router.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

An IPv4 address must be configured for an IPv4 virtual router before the virtual router can be enabled (not required to enable an IPv6 virtual router).

Examples

```
-> ip vrrp 23 interface ipv4-100 address 192.168.173.1
-> ip vrrp 23 interface ipv4-100 address 192.168.173.2
-> ip vrrp 23 interface ipv4-100 no address 192.168.173.1

-> ipv6 vrrp 33 interface ipv6-200 213:100:1::56
-> ipv6 vrrp 33 interface ipv6-200 213:100:1::57
-> ipv6 vrrp 33 interface ipv6-200 no address 213:100:1::56
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; **interface** parameter added; *vlan_id* and optional **ip** parameter deprecated.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router
show vrrp statistics	Displays statistics about VRRP packets for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
vrrpv3AssociatedIpAddrTable
   vrrpv3AssociatedIpAddrRowStatus
```

vrrp track

Creates a new tracking policy or modifies an existing tracking policy.

ip vrrp track *track_id* **[admin-state [enable | disable] | priority** *priority* **| ipv4-interface** *if_name* | **ipv6-interface** *if_name* **| port** *chassis/slot/port* **| address** *ip_address* **[bfd-state {enable | disable} | delay** *seconds***]]**

no ip vrrp track *track_id*

Syntax Definitions

track_id	The ID of the tracking policy. The valid range is 1–255.
admin-state enable	Enables the tracking policy.
admin-state disable	Disables the tracking policy.
priority	The decrement priority value. A virtual router monitoring this tracking policy will have its priority decremented by this value when the conditional state of the tracking policy entity is down. The valid range is 0–255.
if_name	The name of the IPv4 or IPv6 interface that this policy will track.
chassis	The chassis identifier.
slot/port	The slot/port number that this policy will track.
ip_address	The remote IPv4 or IPv6 address that this policy will track.
bfd-state enable	Enables Bidirectional Forwarding Detection (BFD) for an address tracking policy.*This parameter is not supported on the OmniSwitch 6560*.
bfd-state disable	Disables BFD for an address tracking policy. *This parameter is not supported on the OmniSwitch 6560*.
seconds	The amount of time to wait after a VRRP address track is detected as operationally up and before the associated virtual router's priority value is incremented by the tracking policy's priority value. The valid range is 0–60 seconds.

Defaults

parameter	default
admin-state enable | disable	**enable**
priority	25
bfd-state enable | disable	**disable**
seconds	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a tracking policy.
- Use the **admin-state disable** option to disable the tracking policy, rather than removing it from the switch.
- Registering VRRP with BFD is required at the protocol level before VRRP can interact with BFD. Once VRRP is a registered protocol with BFD, then BFD can be enabled for a specific VRRP address tracking policy.
- Enabling BFD for an address tracking policy requires a Loopback0 interface on the local switch. The IP address of this interface will serve as the source IP address of BFD packets. For more information about configuring a Loopback0 interface, see the "IP Commands" or "IPv6 Commands" chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.
- Configuring the delay time for an IPv4 address or IPv6 address tracking policy helps to prevent the loss of device connectivity that may occur before a virtual router prematurely becomes the master. For example, configuring a delay time allows the switch routing tables to stabilize before the master router resumes the master role.

Examples

```
-> ip vrrp track 2 admin-state enable priority 50 ipv4-interface Marketing
-> ip vrrp track 3 admin-state enable priority 60 ipv6-interface Sales
-> ip vrrp track 2 address 10.1.1.1 bfd-state enable
-> ip vrrp track 3 address 10.1.1.2 delay 30
-> ip vrrp track 4 address 20.1.1.2 bfd-state enable delay 45
-> ip vrrp track 5 address 213:100:1::56 bfd-state enable
-> ip vrrp track 2 address 10.1.1.1 bfd-state disable
-> ip vrrp track 5 address 213:100:1::56 bfd-state disable
-> ip vrrp track 3 admin-state disable
-> no ip vrrp track 2
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **delay** parameter added.

Related Commands

vrrp track-association	Associates a VRRP tracking policy with a virtual router.
vrrp bfd-state	Enables or disables the BFD protocol for VRRP.
show vrrp track	Displays information about tracking policies on the switch.

MIB Objects

```
alaVRRPTrackTable
   alaVrrpTrackId
   alaVrrpTrackState
   alaVrrpTrackAdminState
   alaVrrpTrackPriority
   alaVrrpTrackEntityType
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddrType
   alaVrrpTrackEntityIpAddress
   alaVrrpTrackEntityIpv6Interface
   alaVrrpTrackEntityInterface
   alaVrrpTrackBfdStatus
   alaVrrpTrackDelay
   alaVrrpTrackRowStatus
```

vrrp bfd-state

Enables or disables the registration of VRRP with the BFD protocol.

ip vrrp bfd-state {enable | disable}

Syntax Definitions

enable	Enables BFD for VRRP.
disable	Disables BFD for VRRP.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- BFD interaction with VRRP is supported only for VRRP tracking policies that track a remote IP address.
- BFD must be globally enabled for the switch *and* VRRP must be registered with BFD at the protocol level before VRRP can interact with BFD.

Examples

```
-> ip bfd admin-state enable
-> ip vrrp bfd-state enable
-> ip vrrp bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp track	Configures an address tracking policy.
ip bfd admin-state	Enables or disables the global BFD protocol status for the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router

MIB Objects

```
alaVrrpConfig
   alaVrrpBfdStatus
```

vrrp track-association

Associates an IPv4 or IPv6 VRRP tracking policy with a virtual router.

{ip | ipv6} vrrp *vrid* **interface** *if_name* **track-association** *track_id*

{ip | ipv6} vrrp *vrid* **interface** *if_name* **no track-association** *track_id*

Syntax Definitions

ip	Associates a tracking policy with an IPv4 virtual router.
ipv6	Associates a tracking policy with an IPv6 virtual router.
vrid	The virtual router ID. The valid range is 1–255.
if_name	The name of an existing IPv4 or IPv6 interface on which the virtual router is configured.
track_id	The ID of the tracking policy to associate with the virtual router. The valid range is 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a tracking policy from a virtual router.
- The tracking policy ID must already exist in the switch configuration. Use the **vrrp track** command to create a tracking policy.

Examples

```
-> ip vrrp 23 interface ipv4-100 track-association 1
-> ip vrrp 23 interface ipv4-100 no track-association 1

-> ipv6 vrrp 33 interface ipv6-200 track-association 1
-> ipv6 vrrp 33 interface ipv6-200 no track-association 1
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; **interface** parameter added; *vlan_id* parameter deprecated.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.
vrrp track	Configures a VRRP or VRRP3 tracking policy.
show vrrp track-association	Displays the tracking policies associated with virtual routers.

MIB Objects

```
alaVrrp3AssoTrackTable
   alaVrrp3AssoTrackId
   alaVrrp3TrackRowStatus
```

vrrp delay

Configures the amount of time allowed for routing tables to stabilize before virtual routers are started.

ip vrrp delay *seconds*

Syntax Definitions

seconds	The amount of time after a reboot that virtual routers will wait before they go active. The valid range is 0–180 seconds.

Defaults

parameter	default
seconds	45 seconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to prevent loss of workstation connectivity before a virtual router becomes master.

Examples

```
-> ip vrrp delay 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVRRPConfig
   alaVRRPStartDelay
```

vrrp version

Modifies the default VRRP version assigned to the IPv4 virtual routers on the switch. The VRRP version for IPv6 virtual routers is not configurable (IPv6 virtual routers support only version 3).

ip vrrp version [v2 | v3]

Syntax Definitions

v2	Assigns version 2 by default to IPv4 virtual routers.
v3	Assigns version 3 by default to IPv4 virtual routers.

Defaults

parameter	default
v2 | v3	**v2**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Modifying the default VRRP version will affect the version assigned by default to any new IPv4 virtual routers that are created.
- To apply the new default value to the existing IPv4 virtual routers, first disable the virtual routers, then apply the new default value using the **ip vrrp set version** command and enable the virtual routers again.
- If any of the IPv4 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the **ip vrrp set version** command with the **override** option and enable the virtual routers again.
- There is no interoperability between VRRP version 2 and 3. A version 3 virtual router will not acknowledge version 2 advertisements.

Examples

```
-> ip vrrp version v3
-> ip vrrp version v2

-> ip vrrp admin-state disable
-> ip vrrp set version
-> ip vrrp set version override
-> ip vrrp admin-state enable
```

Release History

Release 8.5R2; command introduced.

Related Commands

vrrp admin-state	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVRRPv3IPv4Config
   alaVRRPv3IPv4DefaultVersion
```

vrrp interval

Modifies the default advertising interval value assigned to the IPv4 or IPv6 virtual routers on the switch.

{ip | ipv6} vrrp interval *centiseconds*

Syntax Definitions

ip	Modifies the default advertising interval value assigned to IPv4 virtual routers.
ipv6	Modifies the default advertising interval value assigned to IPv6 virtual routers.
centiseconds	The default advertising interval for IPv4 or IPv6 virtual routers. The valid range is 1–4095 *centiseconds*.

Defaults

parameter	default
centiseconds	100

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Modifying the default advertising interval value will affect the value assigned by default to any new IPv4 or IPv6 virtual routers that are created.
- To apply the new default value to existing IPv4 or IPv6 virtual routers, first disable the virtual routers, then apply the new default value using the **ip vrrp set interval** or **ipv6 vrrp set interval** command and enable the virtual routers again.
- If any of the IPv4 or IPv6 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the **ip vrrp set interval** or **ipv6 vrrp set interval** command with the **override** option and enable the virtual routers again.

Examples

```
-> ip vrrp interval 50
-> ip vrrp admin-state disable
-> ip vrrp set interval
-> ip vrrp set interval override
-> ip vrrp admin-state enable

-> ipv6 vrrp interval 75
-> ipv6 vrrp admin-state disable
-> ipv6 vrrp set interval
-> ipv6 vrrp set interval override
-> ipv6 vrrp admin-state enable
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

Related Commands

vrrp admin-state	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVRRPv3IPv4Config
   alaVRRPv3IPv4DefaultInterval
alaVRRPv3IPv6Config
   alaVRRPv3IPv6DefaultInterval
```

vrrp priority

Modifies the default priority value assigned to the IPv4 or IPv6 virtual routers on the switch.

{ip | ipv6} vrrp priority *priority*

Syntax Definitions

ip	Modifies the default priority value assigned to IPv4 virtual routers.
ipv6	Modifies the default priority value assigned to IPv6 virtual routers.
priority	The default priority value for the IPv4 or IPv6 virtual routers. The valid range is 1–255.

Defaults

parameter	default
priority	100

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Modifying the default priority value will affect the value assigned by default to any new IPv4 or IPv6 virtual routers that are created.
- To apply the new default value to the existing IPv4 or IPv6 virtual routers, first disable the virtual routers, then apply the new default value using the **ip vrrp set priority** or **ipv6 vrrp set priority** command and enable the virtual routers again.
- If any of the IPv4 or IPv6 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the **ip vrrp set priority** or **ipv6 vrrp set priority** command with the **override** option and enable the virtual routers again.

Examples

```
-> ip vrrp priority 50
-> ip vrrp admin-state disable
-> ip vrrp set priority
-> ip vrrp set priority override
-> ip vrrp admin-state enable

-> ipv6 vrrp priority 75
-> ipv6 vrrp admin-state disable
-> ipv6 vrrp set priority
-> ipv6 vrrp set priority override
-> ipv6 vrrp admin-state enable
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

Related Commands

vrrp admin-state	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVRRPv3IPv4Config
   alaVRRPv3IPv4DefaultPriority
alaVRRPv3IPv6Config
   alaVRRPv3IPv6DefaultPriority
```

vrrp preempt

Modifies the default preempt mode assigned to the IPv4 or IPv6 virtual routers on the switch.

{ip | ipv6} vrrp [preempt | no preempt]

Syntax Definitions

ip	Modifies the default preempt mode assigned to IPv4 virtual routers.
ipv6	Modifies the default preempt mode assigned to IPv6 virtual routers.
preempt	Specifies that a higher priority router may preempt a lower priority master router by default.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router by default.

Defaults

parameter	default
preempt | no preempt	**preempt**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Modifying the default preempt mode will affect the mode assigned by default to any new IPv4 or IPv6 virtual routers that are created.
- To apply the new default value to the existing IPv4 or IPv6 virtual routers, first disable the virtual routers, then apply the new default value using the **ip vrrp set preempt** or **ipv6 vrrp set preempt** command and enable the virtual routers again.
- If any of the IPv4 or IPv6 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the **ip vrrp set preempt** or **ipv6 vrrp set preempt** command with the **override** option and enable the virtual routers again.

Examples

```
-> ip vrrp preempt
-> ip vrrp no preempt

-> ip vrrp admin-state disable
-> ip vrrp set preempt
-> ip vrrp set preempt override
-> ip vrrp admin-state enable

-> ipv6 vrrp preempt
-> ipv6 vrrp no preempt
```

```
-> ipv6 vrrp admin-state disable
-> ipv6 vrrp set preempt
-> ipv6 vrrp set preempt override
-> ipv6 vrrp admin-state enable
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

Related Commands

vrrp admin-state	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVRRPv3IPv4Config
   alaVRRPv3IPv4DefaultPreemptMode
alaVRRPv3IPv6Config
   alaVRRPv3IPv6DefaultPreemptMode
```

vrrp accept

Modifies the default accept mode assigned to the IPv4 (version 3) or IPv6 virtual routers on the switch.

{ip | ipv6} vrrp [accept | no accept]

Syntax Definitions

ip	Modifies the default accept mode assigned to IPv4 virtual routers.
ipv6	Modifies the default accept mode assigned to IPv6 virtual routers.
accept	Specifies that the master router, which is not the IP address owner, will accept the packets addressed to the IP address owner as its own.
no accept	Specifies that the master router, which is not the IP address owner, will not accept the packets addressed to the IP address owner as its own.

Defaults

parameter	default
accept | no accept	**accept**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Modifying the default accept mode will affect the mode assigned by default to any new IPv4 or IPv6 virtual routers that are created.
- To apply the new default accept mode value to the existing IPv4 or IPv6 virtual routers, first disable the virtual routers, then apply the new default value using the **ip vrrp set accept** or **ipv6 vrrp set accept** command and enable the virtual routers again.
- If any of the IPv4 or IPv6 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the **ip vrrp set accept** or **ipv6 vrrp set accept** command with the **override** option and enable the virtual routers again.
- The accept mode is not a configurable option for IPv4 virtual routers running VRRP version 2; this command only applies to IPv4 virtual routers running VRRP version 3 and IPv6 virtual routers.

Examples

```
-> ip vrrp accept
-> ip vrrp no accept

-> ip vrrp admin-state disable
-> ip vrrp set accept
-> ip vrrp set accept override
-> ip vrrp admin-state enable
```

```
-> ipv6 vrrp accept
-> ipv6 vrrp no accept

-> ipv6 vrrp admin-state disable
-> ipv6 vrrp set accept
-> ipv6 vrrp set accept override
-> ipv6 vrrp admin-state enable
```

Release History

Release 8.5R2; command was introduced.

Related Commands

vrrp admin-state	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVRRPv3IPv4Config
   alaVRRPv3IPv4DefaultAcceptMode
alaVRRPv3IPv6Config
   alaVRRPv3IPv6DefaultAcceptMode
```

vrrp admin-state

Changes the administrative status of all the IPv4 or IPv6 virtual routers on the switch.

{ip | ipv6} vrrp admin-state [disable | enable | enable-all]

Syntax Definitions

ip	Changes the administrative status of all IPv4 virtual routers.
ipv6	Changes the administrative status of all IPv6 virtual routers.
disable	Disables all the IPv4 or IPv6 virtual routers on the switch.
enable	Enables the IPv4 or IPv6 virtual routers that have not previously been disabled individually or collectively through the **ip vrrp group all** or **ipv6 vrrp group all** command.
enable-all	Enables all the IPv4 or IPv6 virtual routers on the switch including those virtual routers that have been disabled individually or collectively through the **ip vrrp group all** or **ipv6 vrrp group all** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command changes the administrative status of all the IPv4 or IPv6 virtual routers on the switch by executing a single command.
- This command will not affect the ability to change the administrative status of an individual IPv4 or IPv6 virtual router.

Examples

```
-> ip vrrp admin-state disable
-> ip vrrp admin-state enable
-> ip vrrp admin-state enable-all

-> ipv6 vrrp admin-state disable
-> ipv6 vrrp admin-state enable
-> ipv6 vrrp admin-state enable-all
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

Related Commands

vrrp version	Modifies the default VRRP version assigned to the IPv4 virtual routers on the switch.
vrrp interval	Modifies the default advertising interval value assigned to the virtual routers on the switch.
vrrp priority	Modifies the default priority value assigned to the virtual routers on the switch.
vrrp preempt	Modifies the default preempt mode assigned to the virtual routers on the switch.
vrrp accept	Modifies the default accept mode assigned to the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVRRPv3IPv4Config
   alaVRRPv3IPv4AdminState
alaVRRPv3IPv6Config
   alaVRRPv3IPv6AdminState
```

vrrp set

Applies the global default parameter values to IPv4 or IPv6 virtual routers on the switch. When this command is used, IPv4 or IPv6 virtual routers revert to using the default parameter values.

{ip | ipv6} vrrp set {interval | priority | preempt | accept | version | all | none} [override]

Syntax Definitions

ip	Applies the default parameter values to IPv4 virtual routers.
ipv6	Applies the default parameter values to IPv6 virtual routers.
interval	Sets the VRRP advertisement interval value to the default value.
priority	Sets the priority value to the default value.
preempt	Sets the preempt mode to the default mode.
accept	Sets the accept mode to the default mode.
version	Sets the VRRP version for IPv4 virtual routers to the default value.
all	Sets all the parameters value to the new default value.
none	Resets all the parameter values to their default values.
override	Overrides the specified parameters configured value with the new default value.

Defaults

parameter	default
interval | priority | preempt | accept | version | all	**all**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- All the IPv4 or IPv6 virtual routers must be disabled before using this command.
- When a new IPv4 or IPv6 virtual router is created, pre-defined default values for the advertising interval, priority, preempt mode, accept mode, and version (IPv4 only) parameters are applied to the new virtual router. These default parameter values are configurable. For example, the **ip vrrp interval** or **ipv6 vrrp interval** command is used to change the default interval value that is applied to IPv4 or IPv6 virtual routers.
- When a default parameter value is changed, however, it is not automatically applied to *existing* virtual routers. To apply default values that have changed to existing virtual routers, do the following:

  1. Administratively disable all the virtual routers.
  2. Use the **ip vrrp set** or **ipv6 vrrp set** command to apply the changed parameter value.
  3. Administratively enable all the virtual routers.

- If any of the IPv4 or IPv6 virtual routers are running with their own individually configured value or group value, then that value takes priority over the default parameter value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the **ip vrrp set** or **ipv6 vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> ip vrrp admin-state disable

-> ip vrrp set priority
-> ip vrrp set priority override

-> ip vrrp admin-state enable

-> ipv6 vrrp admin-state disable

-> ipv6 vrrp set interval
-> ipv6 vrrp set interval override

-> ipv6 vrrp admin-state enable
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; **accept** and **version** parameters added.

Related Commands

vrrp version	Modifies the default VRRP version assigned to the IPv4 virtual routers on the switch.
vrrp interval	Modifies the default advertising interval value assigned to the virtual routers on the switch.
vrrp priority	Modifies the default priority value assigned to the virtual routers on the switch.
vrrp preempt	Modifies the default preempt mode assigned to the virtual routers on the switch.
vrrp accept	Modifies the default accept mode assigned to the virtual routers on the switch.
vrrp admin-state	Changes the administrative status of all the virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVRRPv3IPv4Config
   alaVRRPv3IPv4SetParam
   alaVRRPv3IPv4Override
alaVRRPv3IPv6Config
   alaVRRPv3IPv6SetParam
   alaVRRPv3IPv6Override
```

vrrp group

Creates a new IPv4 or IPv6 virtual router group or modifies the configuration parameters of an existing IPv4 or IPv6 virtual router group.

{ip | ipv6} vrrp group *vrgid* **[interval** *centiseconds***] [priority** *priority***] [preempt | no preempt] [accept | no accept] [version {v2 | v3}**

no {ip | ipv6} vrrp group *vrgid*

Syntax Definitions

ip	Configures an IPv4 virtual router group.
ipv6	Configures an IPv6 virtual router group.
vrgid	The virtual router group ID. The valid range is 1–255.
centiseconds	The interval in centiseconds after which the master router will send VRRP advertisements. The valid range is 1–4095 centiseconds.
priority	The default priority value for the virtual router group. The valid range is 1–255.
preempt	Specifies that a higher priority router may preempt a lower priority master router.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router by default.
accept	Specifies that the master router, which is not the IP address owner, will accept the packets addressed to the IP address owner as its own. *This parameter applies only to IPv4 version3 and IPv6 virtual routers.*
no accept	Specifies that the master router, which is not the IP address owner, will not accept the packets addressed to the IP address owner as its own. *This parameter applies only to IPv4 version3 and IPv6 virtual routers.*
v2	Converts an IPv4 VRRP router as a version 2 virtual router. *This parameter applies only to IPv4 virtual routers.*
v3	Converts an IPv4 VRRP router to a version 3 virtual router. *This parameter applies only to IPv4 virtual routers.*

Defaults

parameter	default
centiseconds	100
priority	100
preempt | no preempt	**preempt**
accept | no accept	**accept**
v2 | v3	**v2**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the virtual router group.
- The configuration parameters can be modified at any time, but will not have any effect on the virtual routers in the group until the virtual routers are enabled again. To apply the group default values to the virtual routers in a group, you must first disable the virtual router group, then apply the group default value using the **ip vrrp group set** or **ipv6 vrrp group set** command and enable the virtual router group again.
- If any of the virtual routers in the group are running with their individually configured value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual router group, then override the configured value by using the **ip vrrp group set** or **ipv6 vrrp group set** command with the **override** option and enable the virtual router group again.
- When a virtual router group is deleted, the virtual routers assigned to the group become unassigned. However, this does not have any impact on the virtual routers.

Examples

```
-> ip vrrp group 25 interval 50 priority 50 no preempt version v3
-> no ip vrrp group 25

-> ipv6 vrrp group 30 interval 200 priority 75 preempt no accept
-> no ipv6 vrrp group 30
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; **accept** and **version** parameters added.

Related Commands

vrrp group admin-state	Changes the administrative status of all the virtual routers in a virtual router group using a single command.
vrrp group set	Sets the new modified default value to all the virtual routers in a virtual router group.
vrrp group-association	Adds a virtual router to a virtual router group.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

```
alaVrrpv3GroupTable
   alaVrrpv3GroupId
   alaVrrpv3GroupInterval
   alaVrrpv3GroupPriority
   alaVrrpv3GroupPreemptMode
   alaVrrpv3GroupAcceptMode
   alaVrrpv3GroupVersion
   alaVrrpv3GroupRowStatus
```

vrrp group admin-state

Changes the administrative status of all the IPv4 or IPv6 virtual routers in an IPv4 or IPv6 virtual router group using a single command.

{ip | ipv6} vrrp group *vrgid* **admin-state [disable | enable | enable-all]**

Syntax Definitions

ip	Changes the administrative status of all IPv4 virtual routers in the IPv4 group.
ipv6	Changes the administrative status of all IPv6 virtual routers in the IPv6 group.
vrgid	The virtual router group ID. The valid range is 1–255.
disable	Disables all the virtual routers in the group.
enable	Enables those virtual routers that have not previously been disabled individually in the group.
enable-all	Enables all the virtual routers in the group including those virtual routers that have been disabled individually.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If an IPv4 or IPv6 virtual router in a group is disabled on an individual basis, it can only be re-enabled by using the **enable-all** option in this command.
- This command will not affect the ability to change the administrative status of an individual IPv4 or IPv6 virtual router.

Examples

```
-> ip vrrp group 25 admin-state disable
-> ip vrrp group 25 admin-state enable
-> ip vrrp group 25 admin-state enable-all

-> ipv6 vrrp group 30 admin-state disable
-> ipv6 vrrp group 30 admin-state enable
-> ipv6 vrrp group 30 admin-state enable-all
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

Related Commands

vrrp group	Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
vrrp group set	Sets the new modified default value to all the virtual routers in a virtual router group.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

```
alaVrrpv3GroupTable
   alaVrrpv3GroupAdminState
```

vrrp group set

Applies the group default parameter values to all virtual routers in an IPv4 or IPv6 virtual router group. When this command is used, IPv4 or IPv6 virtual routers revert to using the group default parameter values.

{ip | ipv6} vrrp group *vrgid* **set [interval | priority | preempt | accept | version | all] [override]**

Syntax Definitions

ip	Applies the default parameter values to IPv4 virtual routers.
ipv6	Applies the default parameter values to IPv6 virtual routers.
vrgid	The virtual router group ID, in the range from 1–255.
interval	Sets the VRRP advertisement interval value to the default value.
priority	Sets the priority value to the default value.
preempt	Sets the preempt mode to the default mode.
accept	Sets the accept mode to the default mode.
version	Sets the VRRP version for IPv4 virtual routers to the default value.
all	Sets all the parameters' value to the new default value.
override	Overrides the parameter's configured value with the group default value.

Defaults

parameter	default
interval | priority | preempt | accept | version | all	**all**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- All the virtual routers in an IPv4 or IPv6 group must be disabled before using this command.
- To apply the group default value to the virtual routers in a group, first disable the virtual router group, then apply the group default value using the **ip vrrp group set** or **ipv6 vrrp group set** command and enable the virtual router group again.
- If any of the virtual routers in the group are running with their own configured parameter value, then that value will take priority over the group default value. To override the configured value with the group default value, first disable the virtual router group, then override the configured value by using the **ip vrrp group set** or **ipv6 vrrp group set** command with the **override** option and enable the virtual router group again.

Examples

```
-> ip vrrp group 10 admin-state disable
-> ip vrrp group 10 set priority
-> ip vrrp group 10 set priority override
-> ip vrrp group 10 admin-state disable

-> ipv6 vrrp group 20 admin-state disable
-> ipv6 vrrp group 20 set interval
-> ipv6 vrrp group 20 set interval override
-> ipv6 vrrp group 20 admin-state enable
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; **accept** and **version** parameters added.

Related Commands

vrrp group	Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
vrrp group admin-state	Changes the administrative status of all the virtual routers in a virtual router group using a single command.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

```
alaVrrpv3GroupTable
   alaVrrpv3GroupSetParam
   alaVrrpv3GroupOverride
```

vrrp group-association

Adds an IPv4 or IPv6 virtual router to an IPv4 or IPv6 virtual router group.

{ip | ipv6} vrrp *vrid* **interface** *if_name* **group-association** *vrgid*

{ip | ipv6} vrrp *vrid* **interface** *if_name* **no group-association** *vrgid*

Syntax Definitions

ip	Adds an IPv4 virtual router to an IPv4 virtual router group.
ipv6	Adds an IPv6 virtual router to an IPv6 virtual router group.
vrid	The virtual router ID. The valid range is 1–255.
if_name	The name of an existing IPv4 or IPv6 interface on which the virtual router is configured.
vrgid	An existing virtual router group ID. The valid range is 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the IPv4 or IPv6 virtual router from the virtual router group.
- It is not necessary to disable an IPv4 or IPv6 virtual router before adding the virtual router to a group. However, the virtual router will not adopt the group's default parameter values until it is re-enabled.
- It is not necessary to disable an IPv4 or IPv6 virtual router before removing the virtual router from a group.
- Create separate groups for each combination of protocol and version. For example, if IPv4 group 10 specifies VRRP version 2, then only assign IPv4 version 2 virtual routers to group 10.
  - The first virtual router assigned to the group will determine the protocol and version of the group.
  - IPv6 virtual router groups will always be version 3.
  - IPv4 version 3 virtual routers cannot be assigned to a version 2 group and vice versa. However, the version for an IPv4 group can be changed.

Examples

```
-> ip vrrp 25 interface ipv4-100 group-association 10
-> ip vrrp 25 interface ipv4-100 no group-association 10

-> ipv6 vrrp 30 interface ipv6-200 group-association 20
-> ipv6 vrrp 30 interface ipv6-200 no group-association 20
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support and **interface** parameter added; *vlan_id* parameter deprecated.

Related Commands

show vrrp group-association Displays the virtual routers that are associated with a group.

MIB Objects

```
alaVrrpv3AssoGroupTable
   alaVrrpv3AssoGroupRowStatus
```

show vrrp

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

show {ip | ipv6} vrrp [*vrid***]**

Syntax Definitions

ip	Displays the IPv4 virtual router configuration.
ipv6	Displays the IPv6 virtual router configuration.
vrid	The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **show ip vrrp** command to display information about configuration parameters, which may be set through the **ip vrrp** command. Use the **show ip vrrp statistics** command to get information about IPv4 VRRP packets.
- Use the **show ipv6 vrrp** command to display information about configuration parameters, which may be set through the **ipv6 vrrp** command. Use the **show ipv6 vrrp statistics** command to get information about IPv6 VRRP packets.

Examples

```
-> show ip vrrp
VRRP default advertisement interval: 100 centiseconds
VRRP default priority: 100
VRRP default preempt: Yes
VRRP default accept: Yes
VRRP default version: V2
VRRP startup delay: 45  (expired)
VRRP BFD-STATE : Disabled

        Interface        IPv4             Admin                                Adv.
VRID      Name        Address(es) Version Status   Priority Preempt Accept Interval
----+-------------+-------------+-------+--------+--------+-------+------+--------
  10 ipv4-100       192.60.170.2    V2    Disabled      100     Yes     NA      100
                    192.60.170.3
  20 ipv4-200       30.3.3.1        V2    Enabled       100     Yes     NA      100

-> show ip vrrp 10
Virtual Router VRID = 10 on INTERFACE = ipv4-100
  Version       = V2
  Admin. Status = Disabled
  Priority      = 100
```

```
  Preempt       = Yes
  Adv. Interval = 100
  Virtual MAC   = 00-00-5E-00-01-0A
  IP Address(es)
    192.60.170.2
    192.60.170.3

-> show ipv6 vrrp
VRRP default advertisement interval: 100 centiseconds
VRRP default priority: 100
VRRP default preempt: Yes
VRRP default accept: Yes
VRRP startup delay: 50  (expired)
VRRP BFD-STATE : Disabled

        Interface                          Admin                                  Adv.
VRID      Name    IPv6 Address(es)         Status   Priority Preempt Accept Interval
----+-----------+----------------------+--------+--------+-------+------+--------
  1  ipv6-100     fe80::200:5eff:fe00:201  Enabled      100     Yes    Yes      100
  2  ipv6-200     fe80::200:5eff:fe00:202  Enabled      100     Yes    Yes      100
  3  ipv6-300     fe80::200:5eff:fe00:203  Enabled      100     Yes    Yes      100
  4  ipv6-400     fe80::200:5eff:fe00:204  Enabled      100     Yes    Yes      100

-> show ipv6 vrrp 3
Virtual Router VRID = 3 on INTERFACE = ipv6-300
  Version       = V3
  Admin. Status = Enabled
  Priority      = 100
  Preempt       = Yes
  Accept        = Yes
  Adv. Interval = 100
  Virtual MAC   = 00-00-5E-00-02-36
  IP Address(es)
    fe80::200:5eff:fe00:203
```

output definitions

VRRP default advertisement interval	The default advertising interval for all virtual routers on the switch. Configured through the **vrrp interval** command.
VRRP default priority	The default priority value for all virtual routers on the switch. Configured through the **vrrp priority** command.
VRRP default preempt	The default preempt mode for all virtual routers on the switch. Configured through the **vrrp preempt** command.
VRRP default accept	The default accept mode for all virtual routers on the switch. Configured through the **vrrp accept** command.
VRRP default version	The default VRRP version assigned to all IPv4 virtual routers. IPv6 virtual routers support only version 3. Configured through the **vrrp version** command.
VRRP startup delay	The amount of time after a reboot that virtual routers will wait before they go active; allows time for routing tables to stabilize. Configured through the **vrrp delay** command.
VRRP BFD-STATUS	Indicates whether or not (**Enabled** or **Disabled**) VRRP is registered to interact with the Bidirectional Forwarding Detection (BFD) protocol. Configured through the **vrrp bfd-state** command.

output definitions (continued)

VRID	Virtual router identifier. Configured through the **vrrp** command.
Interface Name	The IPv4 or IPv6 interface associated with the VRRP instance. Configured through the **vrrp** command.
IPv4 Address(es) **IPv6 Address(es)**	The assigned IPv4 or IPv6 addresses. Configured through the **vrrp address** command.
Version	The VRRP version assigned to the virtual router (**V2** or **V3**). Configured for IPv4 virtual routers through the **vrrp** command. This value is always set to **V3** for IPv6 virtual routers.
Admin Status	The administrative status of this virtual router instance (**Enabled** allows the virtual router instance to operate; **Disabled** disables the virtual router instance without deleting it). Configured through the **vrrp** command.
Priority	Indicates the VRRP router's priority for the virtual router. Configured through the **vrrp** command.
Preempt	Indicates whether or not (**Yes** or **No**) a higher priority virtual router will preempt a lower priority master router: preempt indicates that a higher priority virtual router will preempt a lower priority master; no preempt indicates that the first backup router to take over for the master will not be preempted by a virtual router with a higher priority. In either case, the IP address owner will always take over it if is available. Configured through the **vrrp** command.
Accept	Indicates whether or not (**Yes** or **No**) a master router that is not the IP address owner will accept packets addressed to the IP address owner as its own. Configured through the **vrrp** command. *This parameter applies only to IPv4 version 3 and IPv6 virtual routers.*
Adv. Interval	Indicates the time interval (in centiseconds) between sending advertisement messages. Only the master router sends advertisements. Configured through the **vrrp** command.
Virtual MAC	Displays the virtual MAC address for the virtual router. • The first 5 bytes for IPv4 and IPv6 version 3 virtual routers is always 00-00-5E-00-02. • The first 5 bytes for IPv4 version 2 virtual routers is always 00-00-5E-00-01. • The last byte indicates the VRID.

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; "VLAN" field replaced with "Interface Name" field; "Accept" and "Version" fields added.

Related Commands

show vrrp statistics	Displays statistics for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
vrrpv3OperationsTable
   vrrpv3OperationsVrId
   vrrpv3OperationsInetAddrType
   vrrpv3OperationsMasterIpAddr
   vrrpv3OperationsRowStatus
   vrrpv3OperationsPriority
   vrrpv3OperationsPreemptMode
   vrrpv3OperationsAcceptMode
   vrrpv3OperationsAdvInterval
alaVrrpv3OperationsExTable
   alaVrrpv3OperVersion
```

show vrrp statistics

Displays statistics about VRRP packets for all virtual routers configured on the switch or for a specific virtual router.

show {ip | ipv6} [*vrid*] statistics

Syntax Definitions

ip	Displays VRRP packet statistics for IPv4 virtual routers.
ipv6	Displays VRRP packet statistics for IPv6 virtual routers.
vrid	The virtual router ID. The valid range is 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **show ip vrrp statistics** command to display information about IPv4 VRRP packets. Use the **show ip vrrp** command to display information about the IPv4 virtual router configuration.
- Use the **show ipv6 vrrp statistics** command to display information about IPv6 VRRP packets. Use the **show ipv6 vrrp** command to display information about the IPv6 virtual router configuration.

Examples

```
-> show ip vrrp statistics
Checksum Errors :          0,
Version Errors  :          0,
VRID Errors     :          0

                Interface
VRID              Name                  State      UpTime   Become Master Adv. Rcvd
----+-------------------------------+----------+----------+-------------+----------
   1 ipv4-100                       Master         378890             1          0
   2 ipv4-15                        Backup           4483             0         44
   7 ipv4-200                       Initialize          0             0          0

-> show ipv6 vrrp statistics
Checksum Errors :          0,
Version Errors  :          0,
VRID Errors     :          0

                Interface
VRID              Name                  State      UpTime   Become Master Adv. Rcvd
----+-------------------------------+----------+----------+-------------+----------
   1  ipv6-101                      Master           2983            1           0
   2  ipv6-102                      Master          60675            1           0
   3  ipv6-103                      Master          60675            1           0
```

output definitions

Checksum Errors	The total number of VRRP packets received with an invalid checksum value.
Version Errors	The total number of VRRP packets received with an invalid version number.
VRID Errors	The total number of VRRP packets received with invalid VRIDs.
VRID	The virtual router identifier.
Interface Name	The name of the IPv4 or IPv6 interface associated with the VRRP instance.
State	The operational state of the VRRP router instance: • **initialize—**the interface is either disabled or down, or the startup delay timer has not expired. • **backup**—this instance is monitoring the availability and state of the master router. • **master**—this instance is functioning as the master router.
UpTime	Time interval (in hundredths of a second) since this virtual router was last initialized.
Become Master	The total number of times this virtual router's state has transitioned from backup to master.
Adv. Rcvd	The total number of VRRP advertisements received by this instance.

```
-> show ip vrrp 1 statistics
Virtual Router VRID = 1 on INTERFACE = ipv4-100,
   State                                = Master,
   UpTime (1/100th second)              = 378890,
   Become master                        = 1,
   Advertisements received              = 0,
   Type errors                          = 0,
   Advertisement interval errors        = 0,
   IP TTL errors                        = 0,
   IP address list errors               = 0,
   Packet length errors                 = 0,
   Zero priority advertisements sent    = 0,
   Zero priority advertisements received  = 0,
   New Master Reason                     = 0,
   Protocol Error Reason                 = 0,
   Discontinuity Time                    = 0,
   Refresh Rate (milliseconds)           = 1000

-> show ipv6 vrrp 5 statistics
Virtual Router VRID = 3 on INTERFACE = ipv6-103,
   State                                = Master,
   UpTime (1/100th second)              = 60675,
   Become master                        = 1,
   Advertisements received              = 0,
   Type errors                          = 0,
   Advertisement interval errors        = 0,
   IP TTL errors                        = 0,
   IP address list errors               = 0,
   Packet length errors                 = 0,
   Zero priority advertisements sent    = 0,
   Zero priority advertisements received  = 0,
   New Master Reason                     = 0,
```

```
Protocol Error Reason                  = 0,
Discontinuity Time                     = 0,
Refresh Rate (milliseconds)            = 1000
```

output definitions

VRID	The virtual router identifier.
INTERFACE	The name of the IPv4 or IPv6 interface associated with the VRRP instance.
State	The operational state of the VRRP router instance: • **initialize—**the interface is either disabled or down, or the startup delay timer has not expired. • **backup**—this instance is monitoring the availability of the master router. • **master**—this instance is functioning as the master router.
UpTime	Time interval (in hundredths of a second) since this virtual router was last initialized.
Become master	The total number of times this virtual router's state has transitioned from backup to master.
Advertisements received	The total number of VRRP advertisement packets received by this instance.
Type errors	The total number of VRRP packets received with an invalid value in the VRRP type field.
Advertisement interval errors	The total number of VRRP packets received in which the advertisement interval differs from the one configured for the virtual router.
IP TTL errors	The total number of VRRP packets received with a TTL (Time-To-Live) value other than 255.
IP address list errors	The total number of VRRP packets in which the IP address list does not match the configured list for the virtual router.
Packet length errors	The total number of VRRP packets received with a length less than the length of the VRRP header.
Zero priority advertisements sent	The total number of VRRP advertisements with a priority of 0 sent by the virtual router.
Zero priority advertisements received	The total number of VRRP advertisements with a priority of 0 received by the virtual router.
New Master Reason	The reason the virtual router transitioned to master state. A value of 0 indicates that the virtual router never transitioned to a master state.
Protocol Error Reason	The reason for the last protocol error. A value of 0 indicates that no protocol errors have occurred.
Discontinuity Time	Indicates what the system up time value was when one or more of the statistics counters experienced a discontinuity. A value of 0 indicates that no discontinuities have occurred since the last reboot.
Refresh Rate (milliseconds)	The minimum polling time interval required to update statistics counters.

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; “VLAN” field replaced with “Interface Name” field; “New Master Reason”, “Protocol Error Reason”, “Discontinuity Time”, and “Refresh Rate” fields added.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
vrrpv3OperationsTable
   vrrpv3OperationsVrId
   vrrpv3OperationsInetAddrType
   vrrpv3OperationsStatus
   vrrpv3OperationsUpTime
vrrpv3Statistics
   vrrpv3RouterChecksumErrors
   vrrpv3RouterVersionErrors
   vrrpv3RouterVrIdErrors
vrrpv3StatisticsTable
   vrrpv3StatisticsMasterTransitions
   vrrpv3StatisticsRcvdAdvertisements
   vrrpv3StatisticsAdvIntervalErrors
   vrrpv3StatisticsIpTtlErrors
   vrrpv3StatisticsRcvdPriZeroPackets
   vrrpv3StatisticsSentPriZeroPackets
   vrrpv3StatisticsRcvdInvalidTypePackets
   vrrpv3StatisticsAddressListErrors
   vrrpv3StatisticsPacketLengthErrors
   vrrpv3StatisticsNewMasterReason
   vrrpv3StatisticsProtoErrReason
   vrrpv3StatisticsRowDiscontinuityTime
   vrrpv3StatisticsRefreshRate
```

show vrrp track

Displays information about tracking policies on the switch.

show ip vrrp track [*track_id***]**

Syntax Definitions

track_id	The ID of the tracking policy to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enter the tracking ID to display information about a particular policy; if no tracking policy ID is entered, information for all tracking policies is displayed.

Examples

```
-> show ip vrrp track
Track                                          Admin    Oper          BFD
 ID                  Policy                    State    State  Pri   Status
-----+-----------------------------------+----------+------+-----+---------
   1    PORT 1/1/1                        Enabled    Up      25   Enabled
   2    192.10.150.42                     Enabled    Down    25   Disabled
   3    INTF02-01                         Enabled    Up      25   Enabled

-> show ip vrrp track 2
Tracking Policy TRACKID = 2
  Policy        = 192.10.150.42
  Dec. Priority = 25
  Admin. Status = Enabled
  Oper. Status  = Down
  BFD  Status   = Disabled
  Delay: 0
```

output definitions

Track ID	The ID of the tracking policy.
Policy	The IP interface, chassis/slot/port, or IP address tracked by the policy.
Dec. Priority	The value to be decremented from the priority value of the virtual router monitoring this tracking policy when the operational state of the tracking policy is down.
Admin. Status	Whether the tracking policy is administratively **Enabled** or **Disabled**.
Oper. Status	Indicates whether the operating state of the tracking policy is **Up** or **Down**.

output definitions

BFD Status	The status (**Enabled** or **Disabled**) of Bidirectional Forwarding Detection (BFD) interaction with the VRRP tracking policy.
Delay	The amount of time, in seconds, to wait after a VRRP address track is detected as operationally up and before the associated virtual router's priority value is incremented by the tracking policy's priority value.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **Delay** field added.

Related Commands

vrrp track	Creates a new tracking policy or modifies an existing tracking policy.
show vrrp track-association	Displays the tracking policies associated with virtual routers

MIB Objects

```
alaVRRPTrackTable
   alaVrrpTrackId
   alaVrrpTrackAdminState
   alaVrrpTrackPriority
   alaVrrpTrackState
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddrType
   alaVrrpTrackEntityIpAddr
   alaVrrpTrackEntityInterface
   alaVrrpTrackEntityIpv6Interface
   alaVrrpTrackBfdStatus
   alaVrrpTrackDelay
```

show vrrp track-association

Displays the tracking policies associated with virtual routers.

show {ip | ipv6} [*vrid***] track-association [***track_id***]**

Syntax Definitions

ip	Displays the tracking policies associated with IPv4 virtual routers.
ipv6	Displays the tracking policies associated with IPv6 virtual routers.
vrid	The virtual router ID. The valid range is 1–255.
track_id	The ID of the tracking policy to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If a track ID is specified, only information about that track ID is displayed. If the virtual router ID and track ID are not specified, information about all virtual routers and their associated tracking policies is displayed.

Examples

```
-> show ip vrrp track-association
      Interface Conf  Cur  Track                          Admin      Oper  Track
VRID    Name    Pri   Pri   ID      Policy                State      State  Pri
----+----------+-----+-----+-----+------------------------+----------+-----+------
   1  IPV4-100  200   175     1   192.168.170.1            Enabled     Up    10
                              3   INTF02-01                Enabled   Down    25
   2  IPV4-200  200   200     1   192.168.170.1            Enabled     Up    10

-> show ip vrrp 1 track-association
      Interface Conf  Cur  Track                          Admin      Oper  Track
VRID    Name    Pri   Pri   ID      Policy                State      State  Pri
----+----------+-----+-----+-----+------------------------+----------+-----+------
   1  IPV4-100  200   175     1   192.168.170.1            Enabled     Up    10
                              3   INTF02-01                Enabled   Down    25

-> show ip vrrp track-association 1
      Interface Conf  Cur  Track                          Admin      Oper  Track
VRID    Name    Pri   Pri   ID      Policy                State      State  Pri
----+----------+-----+-----+-----+------------------------+----------+-----+------
  1  IPV4-100  200   175     1   192.168.170.1            Enabled     Up    10
  2  IPV4-200  200   200     1   192.168.170.1            Enabled     Up    10
```

```
-> show ipv6 vrrp track-association
      Interface Conf  Cur  Track                          Admin      Oper  Track
VRID    Name    Pri   Pri   ID      Policy                 State      State  Pri
----+----------+-----+-----+-----+-----------------------+----------+-----+------
   1 ipv6-250   101   200    1    PORT 1/1/37             Enabled    Up    25
   2 ipv6-300   100   100    2    INTF02-02               Enabled    Up    25
                             3    10.255.11.101           Enabled    Up    25

-> show ipv6 vrrp 2 track-association
      Interface Conf  Cur  Track                          Admin      Oper  Track
VRID    Name    Pri   Pri   ID      Policy                 State      State  Pri
----+----------+-----+-----+-----+-----------------------+----------+-----+------
   2 ipv6-300   100   100    2    INTF02-02               Enabled    Up    25
                             3    10.255.11.101           Enabled    Up    25

-> show ipv6 vrrp track-association 3
      Interface Conf  Cur  Track                          Admin      Oper  Track
VRID    Name    Pri   Pri   ID      Policy                 State      State  Pri
----+----------+-----+-----+-----+-----------------------+----------+-----+------
   2 ipv6-300   100   100    3    10.255.11.101           Enabled    Up    25
```

output definitions

VRID	The virtual router identifier.
Interface Name	The name of the IPv4 or IPv6 interface associated with the virtual router.
Conf Pri	The priority configured for the virtual router.
Cur Pri	The current priority for the virtual router. If the tracking policy is in effect because the tracked entity is down, the current priority will be equal to the configured priority (Conf Pri) minus the tracking priority (Track Pri). Otherwise, the current priority will be equal to the configured priority.
Track ID	The ID of the tracking policy.
Policy	The IPv4 interface, IPv6 interface, port, IPv4 address, or IPv6 address that this policy is tracking.
Admin State	The administrative status (**Enabled** or **Disabled**) of the tracking policy.
Oper State	The operational status (**Up** or **Down**) of the tracking policy.
Track Pri	The amount to be decremented from the configured virtual router priority when the tracking policy is applied.

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; “VLAN” field replaced with “Interface Name” field.

Related Commands

vrrp track-association	Associates a VRRP tracking policy with a virtual router.
vrrp track	Creates a new tracking policy or modifies an existing tracking policy.
show vrrp track	Displays information about tracking policies on the switch
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
vrrpOperTable
   vrrpOperPriority
vrrpv3OperationsTable
   vrrpv3OperationsVrId
   vrrpv3OperationsInetAddrType
alaVrrpv3OperationsExTable
   alaVrrpv3CurrentPriority
alaVrrpAssoTrackTable
   alaVrrpAssoTrackId
alaVRRPTrackTable
   alaVrrpTrackId
   alaVrrpTrackAdminState
   alaVrrpTrackPriority
   alaVrrpTrackState
   alaVrrpTrackEntityPort
   alaVrrpTrackEntityIpAddrType
   alaVrrpTrackEntityIpAddr
   alaVrrpTrackEntityInterface
   alaVrrpTrackEntityIpv6Interface
```

show vrrp group

Displays the default parameter values for all the virtual router groups or for a specific virtual router group.

show {ip | ipv6} vrrp group [*vrgid***]**

Syntax Definitions

ip	Displays the IPv4 virtual routers that belong to a group.
ipv6	Displays the IPv6 virtual routers that belong to a group.
vrgid	The virtual router group ID, in the range from 1–255.

Defaults

By default, the default parameter values are displayed for all the virtual router groups.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the *vrgid* parameter with this command to display the default values for a specific virtual router group.

Examples

```
-> show ip vrrp group
Group   Adv               Preempt   Accept
 ID   Interval  Priority    Mode     Mode   Version
-----+--------+----------+--------+--------+-------
  10    200        75       Yes      No       V3
  20    150        75       Yes      No       V2

-> show ip vrrp group 20
Virtual Router Group GROUPID = 20
  Interval = 150
  Priority = 75
  Preempt Mode = Yes
  Accept Mode = No
  Version = V2
  2 Associated Virtual Routers

-> show ipv6 vrrp group
Group   Adv               Preempt   Accept
 ID   Interval  Priority    Mode     Mode   Version
-----+--------+----------+--------+--------+-------
  30    100        75       Yes      No       V3
  40    125        75       Yes      Yes      V3

-> show ipv6 vrrp group 30
Virtual Router Group GROUPID = 30
  Interval = 100
  Priority = 75
```

```
Preempt Mode = Yes
Accept Mode = No
Version = V3
2 Associated Virtual Routers
```

output definitions

Group ID	The virtual router group identifier.
Adv Interval	The default advertisement time interval, in centiseconds, for the VRRP group. Only the master router sends advertisements.
Priority	The default priority value for the VRRP group.
Preempt Mode	The default preempt mode (**Yes** or **No**) for the VRRP group.
Accept Mode	The default accept mode (**Yes** or **No**) for the VRRP group.
Version	The default VRRP version (**V2** or **V3**) for an IPv4 VRRP group. IPv6 virtual routers support only version 3, so IPv6 VRRP groups are automatically set to V3.

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; “Accept Mode” and “Version” parameters added.

Related Commands

vrrp group	Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
vrrp group admin-state	Changes the administrative status of all the virtual routers in a virtual router group using a single command.

MIB Objects

```
alaVrrpv3GroupTable
   alaVrrpv3GroupId
   alaVrrpv3GroupInterval
   alaVrrpv3GroupPriority
   alaVrrpv3GroupPreemptMode
   alaVrrpv3GroupAcceptMode
   alaVrrpv3GroupVersion
```

show vrrp group-association

Displays the virtual routers that are associated with a virtual router group.

show {ip | ipv6} vrrp group-association [*vrgid***]**

Syntax Definitions

ip	Displays the IPv4 virtual routers that belong to a group.
ipv6	Displays the IPv6 virtual routers that belong to a group.
vrgid	The virtual router group ID, in the range from 1–255.

Defaults

By default, all virtual router group associations are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the *vrgid* parameter with this command to display the association details of a specific virtual router group.

Examples

```
-> show ip vrrp group-association
                        Interface
GROUPID VRID              Name                Version
-------+----+--------------------------------+-------
   10     5  ipv4-100                           V2
          6  ipv4-200                           V2
   20    21  ipv4-300                           V3
         22  ipv4-400                           V3

-> show ip vrrp group-association 20
                        Interface
GROUPID VRID              Name                Version
-------+----+--------------------------------+-------
   20    21  ipv4-300                           V3
         22  ipv4-400                           V3

-> show ipv6 vrrp group-association
                        Interface
GROUPID VRID              Name                Version
-------+----+--------------------------------+-------
   30    31  ipv6-500                           V3
         32  ipv6-600                           V3
   40    41  ipv6-700                           V3
         42  ipv6-800                           V3
```

```
-> show ipv6 vrrp group-association 30
                         Interface
GROUPID VRID               Name                 Version
-------+----+---------------------------------+-------
   30    31  ipv6-500                             V3
         32  ipv6-600                             V3
```

output definitions

GROUPID	The virtual router group identifier.
VRID	The virtual router identifier.
Interface Name	The IPv4 or IPv6 interface associated with the VRRP instance.
Version	The VRRP version for the group (**V2** or **V3**)

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; “Interface Name” and “Version” fields added; “VLAN” field deprecated.

Related Commands

vrrp group-association	Adds a virtual router to a virtual router group.

MIB Objects

```
alaVrrpAssoGroupTable
   alaVrrpGroupIdent
   ifIndex
   vrrpOperVrId
alaVrrpv3AssoGroupTable
   alaVrrpv3GroupIdent
   vrrpv3OperationsInetAddrType
   ifIndex
   vrrpv3OperationsVrId
```

26 OSPF Commands

Open Shortest Path First routing (OSPF) is a shortest path first (SPF) or link-state protocol. OSPF is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPF chooses the least-cost path as the best path.

Each participating router distributes its local state (i.e., the router's usable interfaces and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. This database is built from the collected link state advertisements of all routers. Each multi-access network that has at least two attached routers has a designated router and a backup designated router. The designated router floods a link state advertisement for the multi-access network and has other special responsibilities.

OSPF allows collections of contiguous networks and hosts to be grouped together. A group, together with the routers having interfaces to any one of the included networks, is called an *are*a. Each area runs a separate copy of the basic link-state routing algorithm. This means that each area has its own topological database, as explained in the previous section.

The OmniSwitch version of OSPF complies with RFCs 1370, 1850, 2328, 2370, 3101, and 3623.

MIB information for OSPF is as follows:

Filename: ALCATEL-IND1-VIRTUALROUTER-MIB.mib
Module: alcatelIND1VirtualRouterMIB

Filename: ALCATEL-IND1-OSPF-MIB.mib
Module: alcatelIND1OSPFMIB

Filename: OSPF-MIB.mib
Module: OSPF

The following is a list of the commands for configuring OSPF:

Global OSPF Commands	**ip load ospf** **ip ospf admin-state** **ip ospf asbr** **ip ospf exit-overflow-interval** **ip ospf extlsdb-limit** **ip ospf host** **ip ospf mtu-checking** **ip ospf default-originate** **ip ospf route-tag** **ip ospf spf-timer** **ip ospf virtual-link** **ip ospf neighbor** **show ip ospf** **show ip ospf border-routers** **show ip ospf ext-lsdb** **show ip ospf host** **show ip ospf lsdb** **show ip ospf neighbor** **show ip ospf routes** **show ip ospf virtual-link** **show ip ospf virtual-neighbor**
OSPF Area Commands	**ip ospf area** **ip ospf area default-metric** **ip ospf area range** **show ip ospf area** **show ip ospf area range** **show ip ospf area stub**
OSPF Interface Commands	**ip ospf interface** **ip ospf interface admin-state** **ip ospf interface area** **ip ospf interface auth-key** **ip ospf interface auth-type** **ip ospf interface dead-interval** **ip ospf interface hello-interval** **ip ospf interface md5** **ip ospf interface md5 key** **ip ospf interface type** **ip ospf interface cost** **ip ospf interface poll-interval** **ip ospf interface priority** **ip ospf interface retrans-interval** **ip ospf interface transit-delay** **show ip ospf interface** **show ip ospf interface auth-info**
OSPF BFD Commands	**ip ospf bfd-state** **ip ospf bfd-state all-interfaces** **ip ospf interface bfd-state** **ip ospf interface bfd-state drs-only** **ip ospf interface bfd-state all-neighbors**
OSPF Graceful Restart Commands	**ip ospf restart-support** **ip ospf restart-interval** **ip ospf restart-helper admin-state** **ip ospf restart-helper strict-lsa-checking admin-state** **ip ospf restart initiate** **show ip ospf restart**

ip load ospf

Loads the OSPF software on the router.

ip load ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> ip load ospf
```

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaVrConfigTable
   alaVrConfigOspfStatus
```

ip ospf admin-state

Enables or disables the administration status of OSPF on the router.

ip ospf admin-state {enable | disable}

Syntax Definitions

enable	Enables OSPF.
disable	Disables OSPF.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The OSPF protocol must be enabled for it to route traffic.

Examples

```
-> ip ospf admin-state enable
-> ip ospf admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
ospfGeneralGroup
   ospfAdminStat
```

ip ospf asbr

Configures the router as an Autonomous System Border Router (ASBR). A router running multiple protocols or acting as a gateway to other exterior routers is an ASBR.

ip ospf asbr

no ip ospf asbr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Autonomous System Border Routers (ASBRs) are routers that exchange information with routers from another autonomous system (AS).
- The **no** variant of this command removes the ASBR classification of the selected router.

Examples

```
-> ip ospf asbr
-> no ip ospf asbr
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfAsBdRtr
```

ip ospf exit-overflow-interval

This command sets the overflow interval value.

ip ospf exit-overflow-interval *seconds*

Syntax Definitions

seconds	The number of seconds the router waits before attempting to leave the overflow state.

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The overflow interval is the time whereby the routing router will wait before attempting to leave the database overflow state; the interval begins upon the routing router's arrival into this state.
- When the routing router leaves the overflow state, it can once again create non-default and external link state advertisements (LSAs) for autonomous systems (AS).
- Note that the router will not leave the overflow state (until it is restarted) when the overflow interval value is set to 0.

Example

```
-> ip ospf exit-overflow-interval 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays the OSPF status and general configuration parameters.

MIB Objects

```
ospfGeneralGroup
   ospfExitOverflowInterval
```

ip ospf extlsdb-limit

Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.

ip ospf extlsdb-limit *limit*

Syntax Definitions

limit	The maximum number of LSDB entries allowed on the router. The accepted value is any number greater than or equal to 1. If 0 is entered, there is no limit.

Defaults

parameter	default
limit	-1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows you to set a limit to the number of external LSDBs learned by the router. An external LSDB is created when the router learns a link address that exists outside of its Autonomous System (AS).
- When the limit is set, and it is exceeded, older addresses that were previously learned are removed from the routing table to make room for the new external LSDB.

Example

```
-> ip ospf extlsdb-limit 25
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
ospfGeneralGroup
   ospfExtLsdbLimit
```

ip ospf host

Creates and deletes an OSPF entry for directly attached hosts. Allows for the modification of the host parameters of Type of Service (ToS) and metric.

ip ospf host *ip_address* **tos** *tos* **[metric** *metric***]**

no ip ospf host *ip_address* **tos** *tos*

Syntax Definitions

ip_address	The 32-bit IP address in dotted decimal format of the OSPF host. See the example below for more information.
tos	The type of service (ToS) of the specified OSPF host. The valid range is 0- 15. Only ToS value 0 is supported at this time.
metric	The cost metric value assigned to the specified host. The valid range is 0 and up.

Defaults

parameter	default
metric	0

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **no** variant of this command removes the record of the OSPF host.
- Use this command when multiple paths exist to a host. The specified host must be directly attached to the router. ToS routing is the ability to make a forwarding decision based on a destination address and a desired Quality of Service (QoS). ToS routing allows link selection based on QoS when more than one path exists between a source and a destination.A metric value is the cost of all the hops necessary for a packet to reach its destination. Routers use the metric to determine the best possible path.

Examples

```
-> ip ospf host 172.22.2.115 tos 1 metric 10
-> no ip ospf host 172.22.2.115 tos 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf host	Displays information on configured OSPF hosts.

MIB Objects

```
ospfHostTable
   ospfHostStatus
   ospfHostIpAddress
   ospfHostTOS
   ospfHostMetric
```

ip ospf mtu-checking

Enables or disables the use of Maximum Transfer Unit (MTU) checking. The MTU limits the size of a transmitted or received packet.

ip ospf mtu-checking

no ip ospf mtu-checking

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **no** form of this command disables MTU checking.
- This command is used to disable the checking for mismatch of the interface MTU while establishing a neighbor adjacency with a router. MTU mismatch occurs when a router receives packets that contain a larger MTU value than that of the interface on which adjacency is being established. The interface MTU is the largest IP datagram size (in bytes) that the interface can accept.

Examples

```
-> ip ospf mtu-checking
-> no ip ospf mtu-checking
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays the OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfMTUCheck
```

ip ospf default-originate

Configures a default external route into the OSPF routing domain.

ip ospf default-originate {only | always} [metric-type {type1 | type2}] [metric *value***]**

no ip ospf default-originate

Syntax Definitions

only	Advertises only when there is a default route in the routing table**.**
always	Advertises the default route regardless of whether the routing table has a default route.
type1	Sets the external route as type1.
type2	Sets the external route as type2.
value	The metric value.The valid range is 1-65535.

Defaults

parameter	default
type1 | type2	**type2**
value	1

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to delete redistributed default routes.

Examples

```
-> ip ospf default-originate always
-> ip ospf default-originate only metric 10
-> ip ospf default-originate always metric-type type1 metric 5
-> no ip ospf default-originate
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays the OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfDefaultOriginate
   alaOspfDefaultOriginateMetricType
   alaOspfDefaultOriginateMetric
```

ip ospf route-tag

Configures a tag value that is applied to internal routes for potential redistribution.

ip ospf route-tag *tag*

Syntax Definitions

tag	The set tag value. The valid range is 0–2147483647.

Defaults

parameter	default
tag	0

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

A 32-bit value tagged to each OSPF internal route that is redistributed into other routing protocol domains. The lower 16-bits typically indicate the autonomous system number.

Example

```
-> ip ospf route-tag 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfRedistRouteTag
```

ip ospf spf-timer

Configures timers for Shortest Path First (SPF) calculation.

ip ospf spf-timer [delay *delay_seconds***] [hold** *hold_seconds***]**

Syntax Definitions

delay_seconds	Specifies time (from 0 to 65535 seconds) between the reception of an OSPF topology change and the start of an SPF calculation.
hold_seconds	Specifies the minimum time (from 0 to 65535 seconds) between consecutive SPF calculations.

Defaults

parameter	default
delay_seconds	5
hold_seconds	10

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows you to configure the time between SPF calculations. Using the delay timer, you can determine how much time to postpone an SPF calculation after the router receives a topology change. Using the hold timer, you can configure the amount of time that must elapse between consecutive SPF calculations.
- Note that if either of these values is set to 0, there will be no delay in the SPF calculation. This means that SPF calculations will occur immediately upon the reception of a topology change and/or that back-to back SPF calculations can take place with no break in-between the two.

Example

```
-> ip ospf spf-timer delay 20 hold 35
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays the OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
   alaOspfTimerSpfDelay
   alaOspfTimerSpfHold
```

ip ospf virtual-link

Creates or deletes a virtual link. A virtual link is used to restore backbone connectivity if the backbone is not physically contiguous.

ip ospf virtual-link *area_id router_id* **[auth-type {none | simple | md5}] [auth-key** *key_string***] [dead-interval** *seconds***] [hello-interval** *seconds***] [retrans-interval** *seconds***] [transit-delay** *seconds***]**

no ip ospf virtual-link *area_id router_id*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
router_id	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
none	Sets the virtual link authorization type to no authentication.
simple	Sets the virtual link authorization type to simple authentication. If **simple** is selected, a key must be specified as well.
md5	Sets the virtual link authorization type to MD5 authentication.
key_string	Sets the virtual link authorization key. The key can be up to 8 ASCII characters. See the example for more details.
dead-interval *seconds*	Sets the virtual link dead interval. If no hello packets on this link for the set number of seconds have been received, the virtual neighbor is declared dead. The valid range is 1–2147483647.
hello-interval *seconds*	Sets the virtual link hello interval, which is the time interval between OSPF hellos sent on this virtual link. The valid range is 1–65535.
retrans-interval *seconds*	Sets the virtual link retransmit interval. The router waits the set number of seconds before retransmitting OSPF packets. The valid range is 0–3600.
transit-delay *seconds*	Sets the virtual link transit delay, which is the number of seconds to transmit OSPF packets over this link. The valid range is 0–3600.

Defaults

parameter	default
none | simple | md5	**none**
key_string	null string
dead-interval *seconds*	40
hello-interval *seconds*	10
retrans-interval *seconds*	5
transit-delay *seconds*	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The **no** form of the command deletes the virtual link.
- It is possible to define areas in such a way that the backbone is no longer contiguous. In this case the system administrator can ensure backbone connectivity physically.
- Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.
- If authentication is enabled, both routers at either end of the virtual link must share the same password. Simple authentication refers to the use of only clear-text passwords as an authentication method. MD5 authentication refers to the usage of message digests.
- The **dead-interval** value should be the same for all routers on the same network. This value should be some multiple of the value given for the hello interval.

Examples

```
-> ip ospf virtual-link 0.0.0.1 172.22.2.115
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 auth-key "techpubs"
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 auth-type simple
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 dead-interval 50
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 hello-interval 20
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 retrans-interval 20
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 transit-delay 50
-> no ip ospf virtual-link 0.0.0.1 172.22.2.115
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf virtual-link	Displays the virtual link information.

MIB Objects

```
ospfVirtIfTable
   ospfVirtIfAreaId
   ospfVirtIfNeighbor
   ospfVirtIfAuthKey
   ospfVirtIfStatus
   ospfVirtIfAuthType
   ospfVirtIfRtrDeadInterval
   ospfVirtIfHelloInterval
   ospfVirtIfRetransInterval
   ospfVirtIfTransitDelay
```

ip ospf neighbor

Creates a static neighbor on a non-broadcast interface.

ip ospf neighbor *neighbor_id* **{eligible | ineligible}**

no ip ospf neighbor *neighbor_id*

Syntax Definitions

neighbor_id	A unique 32-bit IP address identical to the neighbor's interface address.
eligible	Sets this router as eligible to be the DR.
non-eligible	Sets this router as not eligible to be the DR.

Defaults

parameter	default
eligible | ineligible	**eligible**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- NBMA (Non Broadcast Multi Access), PMP (Point-to-Multipoint), and P2P (Point-to-Point) OSPF non-broadcast modes are supported over Ethernet interfaces (broadcast media).
- Neighboring routers on non-broadcast OSPF networks must be statically configured, because lack of OSPF multicast capabilities prevents using normal OSPF Hello protocol discovery.
- In the case of NBMA interface the static neighbor eligibility for becoming a DR can be configured while it is not necessary for point-to-multipoint and point-to-point interfaces.
- An interface connected to this neighbor must also be configured as a non-broadcast interface, which can be either point-to-multipoint or point-to-point, by using the **ip ospf interface type** command.
- For the correct working of an OSPF NBMA network, a fully meshed network is mandatory. Also, the neighbor eligibility configuration for a router on every other router should match the routers interface priority configuration.

Examples

```
-> ip ospf neighbor 1.1.1.1 ineligible
-> no ip ospf neighbor 1.1.1.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface type	Configures the OSPF interface type.
show ip ospf neighbor	Displays information on OSPF non-virtual neighbor routers.

MIB Objects

```
ospfNbrTable
   ospfNbrPriority
   ospfNbmaNbrStatus
```

ip ospf area

Assigns an OSPF interface to a specified area.

ip ospf area *area_id* **[summary {enable | disable}] | [type {normal | stub | nssa}]**

no ip ospf area *area_id*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
enable	Enables summarization.
disable	Disables summarization.
normal	Sets the area as a regular OSPF area. *This parameter is not supported on an OmniSwitch 6560.*
stub	Configures an OSPF area as a stub area.
nssa	Configures an OSPF area as a Not So Stubby Area (NSSA). *This parameter is not supported on an OmniSwitch 6560.*

Defaults

parameter	default
enable | disable	**enable**
normal | stub | nssa	**normal**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **no** form deletes the area.
- The **summary** options are used to enable or disable route summarization for stub and NSSA areas. Stub and NSSA areas will not receive LSA type 3 unless summary is enabled.
- The **type** command allows you to chose what type of area this is going to be.
- Consider the following when configuring an OSPF area ID on an OmniSwitch 6560:
  - Only one non-zero stub area is supported (configuring a 0.0.0.0 area ID is not allowed).
  - Only two IP OSPF interfaces can be associated with the area.

Examples

```
-> ip ospf area 0.0.0.1
-> ip ospf area 0.0.0.1 type stub
-> ip ospf area 0.0.0.1 type normal
-> no ip ospf area 0.0.0.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area default-metric	Creates or deletes an OSPF default metric.
ip ospf area range	Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
show ip ospf area	Displays either all OSPF areas, or a specified OSPF area.

MIB Objects

```
ospfAreaTable
   ospfImportAsExtern
   ospfAreaSummary
   ospfAreaId
```

ip ospf area default-metric

Creates or deletes a default metric for stub or Not So Stubby Area (NSSA) areas. The default metric configures the type of cost metric that a default area border router (ABR) will advertise in the default summary Link State Advertisement (LSA).

ip ospf area *area_id* **default-metric** *tos* **[[cost** *cost***] | [type {ospf | type 1 | type 2}]**

no ip ospf area *area_id* **default-metric** *tos*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
tos	Type of service. The valid range is 0–15. Only ToS value 0 is supported at this time.
cost	The numerical cost of this area and ToS. Only 0 is supported in the current release.
ospf	Advertises external routes as OSPF autonomous system external (ASE) routes.
type1	Advertises external routes as a Type 1 (non-OSPF) metric.
type2	Advertises external routes as a Type 2 (calculated weight value from non-OSPF protocol) metric.

Defaults

parameter	default
tos	0
ospf | type 1 | type 2	**ospf**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **no** form deletes the default metric from the specified area.
- The **type** command configures the type of cost metric for the specified ToS.To ensure that internal routers receiving external route advertisements choose the correct route, all border routers advertising a particular external network should be configured to advertise the route using the same metric type. That is, they must all advertise the route using an OSPF, Type 1, or Type 2 metric.

Examples

```
-> ip ospf area 1.1.1.1 default-metric 0
-> no ip ospf area 1.1.1.1 default-metric 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area.
ip ospf area range	Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
show ip ospf area	Displays either all OSPF areas, or a specified OSPF area.

MIB Objects

```
ospfStubAreaTable
   ospfStubAreaId
   ospfStubTOS
   ospfStubStatus
   ospfStubMetric
   ospfStubMetricType
```

ip ospf area range

Creates a route summarization instance whereby a range of addresses assigned for the route at the area border router will be advertised.

ip ospf area *area_id* **range {summary | nssa}** *ip_address subnet_mask* **[effect {admatching | noMatching}]**

no ip ospf area *area_id* **range {summary | nssa}** *ip_address subnet_mask*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
summary	Advertises the address range as a summary link state advertisement (LSA).
nssa	Advertises the address range of Not So Stubby Area (NSSA) routes as a Type 5 advertisement. *This parameter is not supported on an OmniSwitch 6560.*
ip_address	A 32-bit IP address for the range's area.
subnet_mask	A 32-bit subnet mask that determines how many bits of the IP address denote the network number.
admatching	Determines that routes specified falling within the specified range will be advertised.
noMatching	Determines that any route falling within the specified range will not be advertised.

Defaults

parameter	default
summary | nssa	**summary**
admatching | noMatching	**admatching**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Route summarization is the consolidation of addresses within an area which are advertised as a single route. When network numbers in an area are assigned consecutively, the area border router can be configured, using this command, to advertise a route that aggregates all the individual networks within the range.
- Using this command causes a single route to be advertised, for an address range in the specified area, to other areas.
- An NSSA (Not So Stubby Area) is similar to a stub area. However, where autonomous system (AS) external routes cannot be imported into a stub area, an NSSA will allow the importing of some AS external routes.

- Area ranges, once created, are enabled by default. Classless Inter-Domain Routing (CIDR) can work with OSPF to make route summarization more efficient. This is especially true for the summarization of routes in the global database. OSPF area address ranges can be configured on area border routers

Examples

```
-> ip ospf area 1.1.1.1 range summary 172.22.2.0 255.255.255.0
-> no ip ospf area 1.1.1.1 range summary 172.22.2.0 255.255.255.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area.
ip ospf area default-metric	Creates or deletes an OSPF default metric.
show ip ospf area range	Displays all or specified route summaries in a given area.

MIB Objects

```
ospfAreaAggregateTable
   ospfAreaAggregateAreaId
   ospfAreaAggregateLsdbType
   ospfAreaAggregateNet
   ospfAreaAggregateMask
   ospfAreaAggregateEffect
   ospfAreaAggregateStatus
```

ip ospf interface

Creates and deletes an OSPF interface.

ip ospf interface {*interface_name***}**

no ip ospf interface {*interface_name***}**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to delete an OSPF interface.
- The interface name cannot contain spaces.

Examples

```
-> ip ospf interface vlan-101
-> no ip ospf interface vlan-101
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfIpAddress
alaOspfIfAugTable
   alaOspfIfIntfName
```

ip ospf interface admin-state

Enables or disables the administrative status on an OSPF interface.

ip ospf interface {*interface_name***} admin-state {enable | disable}**

no ip ospf interface {*interface_name***} admin-state {enable | disable}**

Syntax Definitions

interface_name	The name of the interface.
enable	Enables the OSPF interface.
disable	Disables the OSPF interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to delete an OSPF interface.
- The OSPF interface must be enabled for it to participate in the OSPF protocol.

Examples

```
-> ip ospf interface vlan-101 admin-state enable
-> ip ospf interface vlan-101 admin-state disable
-> no ip ospf interface vlan-101 admin-state enable
-> no ip ospf interface vlan-101 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfAdminStat
```

ip ospf interface area

Configures an OSPF area identifier for this interface.

ip ospf interface {*interface_name***} area** *area_id*

Syntax Definitions

interface_name	The name of the interface.
area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

An interface must be assigned to an area to become operational.

Examples

```
-> ip ospf interface vlan-101 area 0.0.0.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf area	Displays either all the OSPF areas, or a specified OSPF area.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfAreaId
```

ip ospf interface auth-key

Configures an OSPF authentication key for simple authentication on an interface.

ip ospf interface {*interface_name***} auth-key** *key_string*

Syntax Definitions

interface_name	The name of the interface.
key_string	An authentication key (8 characters maximum).

Defaults

The default for the authentication key string is a null string.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Sets a password as a simple text string of 8 ASCII characters.
- Must be used in conjunction with the **auth-type** command, described on page 26-30, set to **simple**.

Examples

```
-> ip ospf interface vlan-101 auth-key pass
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface auth-type	Sets the authentication type.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
  ospfIfAuthKey
```

ip ospf interface auth-type

Sets the OSPF interface authentication type. Authentication allows the router to only respond to other routers that have the correct authentication information.

ip ospf interface {*interface_name***} auth-type {none | simple | md5 | key-chain** *key-chain-id***}**

Syntax Definitions

interface_name	The name of the interface.
none	No authentication.
simple	Simple, clear text authentication.
md5	MD5 encrypted authentication.
key-chain-id	The configured keychain ID.

Defaults

parameter	default
none | simple | md5 | key-chain	**none**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to set the type of authentication that the OSPF interface uses to validate requests for route information from other OSPF neighbors on this interface.
- Simple authentication is authentication that uses only a text string as the password. The authentication type **simple** is used in conjunction with the **auth-key** keyword described, on page 26-29.
- MD5 authentication is encrypted authentication that uses an encryption key string and a key identification number. Both of these are necessary as the password. The authentication type **md5** is used in conduction with the commands described on page 26-34 and page 26-36. One command enables MD5 and the other sets the key identification number.
- Use **keychain** to configure a keychain authentication type for an interface. When the OSPF interface receives a packet, the authentication information is carried in the hello packet. If the authentication succeeds, then adjacency is formed. The two remote machines must have the same active current key ID and same authentication type. Use **ip ospf interface auth-type none** to disassociate the keychain from the interface.

Examples

```
-> ip ospf interface vlan-101 auth-type simple
-> ip ospf interface vlan-101 auth-type key-chain 1
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **key-chain** parameter added.

Related Commands

ip ospf interface auth-key	Sets the password for simple authentication.
show ip ospf interface	Displays the status and statistics of an OSPF interface.
show ip ospf interface auth-info	Displays authentication information for the interface.

MIB Objects

```
ospfIfTable
   ospfIfAuthType
   alaOspfIfKeyChainId
```

ip ospf interface dead-interval

Configures the OSPF interface dead interval.

ip ospf interface {*interface_name***} dead-interval** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The dead interval, in seconds. The valid range is 1–65535.

Defaults

parameter	default
seconds (broadcast and point-to-point)	40
seconds (NBMA and point-to-multipoint)	120

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This is the interval, in seconds, after which a neighbor on this interface is considered dead if no hello packets have been received from this neighbor.
- This interval should be greater than the hello interval or the multiple of the hello interval.

Examples

```
-> ip ospf interface vlan-101 dead-interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface hello-interval	Configures the OSPF interface hello interval.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfRtrDeadInterval
```

ip ospf interface hello-interval

Configures the OSPF interface hello interval.

ip ospf interface {*interface_name***} hello-interval** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The hello interval, in seconds. The valid range is 0–65535. A value of 0 creates a passive OSPF interface.

Defaults

parameter	default
seconds (broadcast and point-to-point)	10
seconds (NBMA and point-to-multipoint)	30

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This is the interval between two consecutive hello packets sent out on this interface.

Examples

```
-> ip ospf interface vlan-101 hello-interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfHelloInterval
```

ip ospf interface md5

Creates and deletes the OSPF interface MD5 key identification number.

ip ospf interface {*interface_name***} md5** *key_id* **[enable | disable]**

Syntax Definitions

interface_name	The name of the interface.
key_id	A key identification number. The key identification number specifies a number that allows MD5 encrypted routers to communicate. Both routers must use the same key ID. The valid range is 1–255.
enable	Enables the interface key.
disable	Disables the interface key.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- MD5 authentication can be used to encrypt information sent over the network. MD5 authentication works by using shared secret keys. Keys are used to sign the packets with an MD5 checksum, and they cannot be forged or tampered with. Since the keys are not included in the packet, snooping the key is not possible.
- This command is used in conjunction with the commands described on page 26-30 and page 26-36.
- The **no** variant deletes the key ID number.

Examples

```
-> ip ospf interface vlan-101 md5 100
-> ip ospf interface vlan-101 md5 10 disable
-> ip ospf interface vlan-101 md5 10 enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface md5 key	Configures the OSPF key ID and key.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
alaOspfIfMd5Table
   alaOspfIfMd5IpAddress
   alaOspfIfMd5KeyId
```

ip ospf interface md5 key

Configures the OSPF key string. This interface MD5 string, along with the key identification number, enables the interface to encode MD5 encryption.

ip ospf interface {*interface_name***} md5** *key_id* **key** *key_string*

Syntax Definitions

interface_name	The name of the interface.
key_id	The key ID. The valid range is 1–255.
key_string	A key string.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used in conjunction with the commands described above on page 26-30 and page 26-34.
- For MD5 authentication to function properly the same key string must be configured on the neighboring router for that interface.

Examples

```
-> ip ospf interface vlan-101 md5 100 key 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface md5	Creates and deletes the OSPF interface MD5 key identification number.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
alaOspfIfMd5Table
   alaOspfIfMd5IpAddress
   alaOspfIfMd5KeyId
   alaOspfIfMd5Key
```

ip ospf interface type

Configures the OSPF interface type.

ip ospf interface {*interface_name***} type {point-to-point | point-to-multipoint | broadcast | non-broadcast}**

Syntax Definitions

interface_name	The name of the interface.
point-to-point	Sets the interface to be a point-to-point OSPF interface.
point-to-multipoint	Sets the interface to be a point-to-multipoint OSPF interface.
broadcast	Sets the interface to be a broadcast OSPF interface.
non-broadcast	Sets the interface to be NBMA (Non Broadcast Multi Access) OSPF interface.

Defaults

parameter	default
broadcast | non-broadcast | point-to-point| point-to-multipoint	**broadcast**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command sets an interface to be broadcast, non-broadcast, point-to-point, or point-to-multipoint.
- If the type is non-broadcast or point-to-multipoint, static neighbors should be configured.

Examples

```
-> ip ospf interface vlan-101 type non-broadcast
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf neighbor	Creates a static neighbor on a Non Broadcast Multi Access (NBMA) interface.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfType
```

ip ospf interface cost

Configures the OSPF interface cost.

ip ospf interface {*interface_name***} cost** *cost*

Syntax Definitions

interface_name	The name of the interface.
cost	The interface cost. The valid range is 0–65535.

Defaults

parameter	default
cost	1

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The configured interface cost, if any, is used during OSPF route calculations.

Examples

```
-> ip ospf interface vlan-101 cost 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfMetricTable
   ospfIfMetricIpAddress
   ospfIfMetricValue
```

ip ospf interface poll-interval

Configures the OSPF poll interval for a Non Broadcast Multi Access (NBMA) interface.

ip ospf interface {*interface_name***} poll-interval** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The poll interval, in seconds. The valid range is 1–2147483647.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This parameter configures the larger time interval, in seconds, between hello packets sent to an inactive neighbor.

Examples

```
-> ip ospf interface vlan-101 poll-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfPollInterval
```

ip ospf interface priority

Configures the OSPF interface priority. The priority number helps determine the eligibility of this router to become the designated router on the network.

ip ospf interface {*interface_name***} priority** *priority*

Syntax Definitions

interface_name	The name of the interface.
priority	The interface priority. The valid range is 0–255.

Defaults

parameter	default
priority	1

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the highest priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become the designated router.

Examples

```
-> ip ospf interface vlan-101 priority 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfRtrPriority
```

ip ospf interface retrans-interval

Configures the OSPF interface retransmit interval.

ip ospf interface {*interface_name***} retrans-interval** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The retransmit interval, in seconds. The valid range 0–3600.

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The number of seconds between link retransmission of OSPF packets on this interface.

Examples

```
-> ip ospf interface vlan-101 retrans-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfRetransInterval
```

ip ospf interface transit-delay

Configures the OSPF interface transit delay.

ip ospf interface {*interface_name***} transit-delay** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The transit delay, in seconds. The valid range is 0–3600.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The estimated number of seconds required to transmit a link state update over this interface. This command takes into account transmission and propagation delays and must be greater than 0.

Examples

```
-> ip ospf interface vlan-101 transit-delay 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable
   ospfIfTransitDelay
```

ip ospf bfd-state

Enables or disables the registration of OSPF with the BFD protocol.

ip ospf bfd-state {enable | disable}

Syntax Definitions

enable	Enables BFD for OSPF.
disable	Disables BFD for OSPF.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- BFD must be globally enabled for the switch and OSPF must be registered with BFD at the protocol level before OSPF can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and the OSPF protocol acts based upon the BFD message.
- Whenever a neighbor goes down, OSPF will inform BFD to remove that neighbor from the BFD active list.

Examples

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of OSPF with the BFD protocol:

```
-> ip ospf bfd-state enable
-> ip ospf bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd admin-state	Enables or disables the global BFD protocol status for the switch.
ip ospf bfd-state all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-state	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
ip ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
show ip ospf	Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolospf
   alaOspfBfdStatus
```

ip ospf bfd-state all-interfaces

Enables or disables BFD for all OSPF interfaces in the switch configuration.

ip ospf bfd-state all-interfaces {enable | disable}

Syntax Definitions

enable	Enables BFD for all the OSPF interfaces.
disable	Disables BFD for all the OSPF interfaces.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf bfd-state all-interfaces enable
-> ip ospf bfd-state all-interfaces disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf bfd-state	Enables or disables the BFD status for the OSPF protocol.
ip ospf interface bfd-state	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
ip ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
show ip ospf interface	Displays configuration information for an OSPF interface.

MIB Objects

```
alaProtocolospf
   alaOspfBfdAllInterfaces
```

ip ospf interface bfd-state

Enables or disables BFD for a specific OSPF interface.

ip ospf interface *if_name* **bfd-state {enable | disable}**

Syntax Definitions

if_name	The name of an existing OSPF interface.
enable	Enables BFD for the OSPF interface.
disable	Disables BFD for the OSPF interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-state enable
-> ip ospf interface int2 bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf bfd-state	Enables or disables the BFD status for the OSPF protocol.
ip ospf bfd-state all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
ip ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
show ip ospf interface	Displays configuration information for an OSPF interface.

MIB Objects

```
alaOspfIfAugEntry
   ospfIfIpAddress
   alaOspfIfBfdStatus
```

ip ospf interface bfd-state drs-only

Establishes BFD sessions only with neighbors that are in the full state.

ip ospf interface *if_name* **bfd-state drs-only**

Syntax Definitions

if_name	The name of an existing OSPF interface.

Defaults

parameter	default
drs-only	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The specified OSPF interface must be enabled to interact with BFD.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-state drs-only
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf bfd-state	Enables or disables the BFD status for OSPF protocol.
ip ospf bfd-state all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-state	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
show ip ospf interface	Displays configuration information for an OSPF interface.

MIB Objects

```
alaOspfIfAugEntry
   ospfIfIpAddress
   alaOspfIfBfdDrsOnly
```

ip ospf interface bfd-state all-neighbors

Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

ip ospf interface *if_name* **bfd-state all-neighbors {enable | disable}**

Syntax Definitions

if_name	The name of an existing OSPF interface.
enable	Enables BFD sessions with all neighbors.
disable	Disables BFD sessions with all neighbors.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The specified OSPF interface must be enabled to interact with BFD.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-state all-neighbors enable
-> ip ospf interface int1 bfd-state all-neighbors disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf bfd-state	Enables or disables the BFD status for OSPF protocol.
ip ospf bfd-state all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-state	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
show ip ospf interface	Displays configuration information for an OSPF interface.

MIB Objects

```
alaOspfIfAugEntry
   ospfIfIpAddress
   alaOspfIfBfdDrsOnly
```

ip ospf restart-support

Configures support for the graceful restart feature on an OSPF router.

ip ospf restart-support {planned-unplanned | planned-only}

no ip ospf restart-support

Syntax Definitions

planned-unplanned	Specifies support for planned and unplanned restarts.
planned-only	This parameter is currently not supported.

Defaults

Graceful restart is disabled be default.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to disable support for the graceful restart feature on an OSPF router.
- The minimum hardware configuration for this command is a redundant CMM configuration.

Examples

```
-> ip ospf restart-support planned-unplanned
-> no ip ospf restart-support
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartSupport
```

ip ospf restart-interval

Configures the grace period for achieving a graceful OSPF restart.

ip ospf restart-interval [*seconds***]**

Syntax Definitions

seconds	The hitless restart timeout interval. The valid range is 0–1800 seconds.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration.

Example

```
-> ip ospf restart-interval 600
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.
show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartInterval
```

ip ospf restart-helper admin-state

Administratively enables and disables the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart.

ip ospf restart-helper [admin-state {enable | disable}]

Syntax Definitions

enable	Enables the capability of an OSPF router to operate in helper mode.
disable	Disables the capability of an OSPF router to operate in helper mode.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration.

Examples

```
-> ip ospf restart-helper admin-state disable
-> ip ospf restart-helper admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.
ip ospf restart-helper strict-lsa-checking admin-state	Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.
show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartHelperSupport
```

ip ospf restart-helper strict-lsa-checking admin-state

Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

ip ospf restart-helper strict-lsa-checking admin-state {enable | disable}

Syntax Definitions

enable	Enables whether or not a changed LSA will result in termination of graceful restart by a helping router.
disable	Disables whether or not a changed LSA will result in termination of graceful restart by a helping router.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration.

Examples

```
-> ip ospf restart-helper strict-lsa-checking admin-state disable
-> ip ospf restart-helper strict-lsa-checking admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.
ip ospf restart-helper admin-state	Administratively enables and disables the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart.
show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartHelperSupport
```

ip ospf restart initiate

Initiates a planned graceful restart.

ip ospf restart initiate

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You must execute this command on the primary CMM before executing a **takeover** command.
- The minimum hardware configuration for this command is a redundant CMM configuration.

Example

```
-> ip ospf restart initiate
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
   alaOspfRestartInitiate
```

show ip ospf

Displays the OSPF status and general configuration parameters.

show ip ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command is used to display the general configuration parameters of the OSPF router. See the Related Commands section below for commands that are used to modify the displayed parameters.

Examples

```
-> show ip ospf
Router Id                       = 10.255.11.242,
OSPF Version Number             = 2,
Admin Status                    = Enabled,
Area Border Router ?            = No,
AS Border Router Status         = Enabled,
Route Tag                       = 0,
SPF Hold  Time (in seconds)     = 10,
SPF Delay  Time (in seconds)    = 5,
MTU Checking                    = Disabled,
# of Routes                     = 124,
# of AS-External LSAs           = 60,
# of self-originated LSAs       = 1,
# of LSAs received              = 118,
External LSDB Limit             = -1,
Exit Overflow Interval          = 0,
# of SPF calculations done      = 38395,
# of Incr SPF calculations done  = 0,
# of Init State Nbrs            = 0,
# of 2-Way State Nbrs           = 0,
# of Exchange State Nbrs        = 0,
# of Full State Nbrs            = 1,
# of attached areas             = 1,
# of Active areas               = 1,
# of Transit areas              = 0,
# of attached NSSAs             = 0,
Default Route Origination       = none,
Default Route Metric-Type/Metric = type2 / 1,
BFD Status                      = Disabled
Opaque Transit Capability       = Enabled
```

output definitions

Router Id	The unique identification for the router.
OSPF Version Number	The version of OSPF the router is running.
Admin Status	Whether OSPF is currently enabled or disabled on the router.
Area Border Router?	Whether the router status is an area router or not.
AS Border Router Status	Whether the area Autonomous System Border Router status of this router is enabled or disabled.
Route Tag	Shows the route tag for this router.
SPF Hold Time	Shows the time in seconds between the reception of an OSPF topology change and the start of a SPF calculation.
SPF Delay Time	Shows the time in seconds between consecutive SPF calculations.
MTU Checking	Shows whether Maximum Transfer Unit checking is enabled or disabled.
# of Routes	The total number of OSPF routes known to this router.
# of AS-External LSAs	The number of external routes learned from outside the router's Autonomous System (AS).
# of self-originated LSAs	The number of times a new Link State Advertisement has been sent from this router.
# of LSAs received	The number of times a new Link State Advertisement has been received by this router.
External LSDB Limit	The maximum number of entries allowed in the external Link State Database.
Exit Overflow Interval	The number of seconds the router remains in the overflow state before attempting to leave it.
# of SPF calculations done	The number of SPF calculations that have occurred.
# of Incr SPF calculations done	The number of incremental SPF calculations done.
# of Init State Nbrs	The number of neighbors in the initialization state.
# of 2-Way State Nbrs	The number of OSPF 2-way state neighbors on this router.
# of Exchange State Nbrs	The number of neighbors in the exchange state.
# of Full State Nbrs	The number of neighbors in the full state.
# of attached areas	The number of areas that are configured on the router.
# of Active areas	The number of areas that are active.
# of Transit areas	The number of transit areas that are configured on the router.
# of attached NSSAs	The number of Not So Stubby Areas that are configured on the router.
Default Route Origination	Whether route redistribution is enabled or disabled on the router.
Default Route Metric-Type/ Metric	The default metric for stub or Not So Stubby Area (NSSA) areas. Specifies the type of cost metric that a default area border router (ABR) will advertise in the default summary Link State Advertisement (LSA).
BFD Status	Whether BFD monitoring is enabled or disabled for OSPF.
Opaque Transit Capability	Whether the opaque LSA accept and retransmit capability for OSPF is enabled or disabled.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip router router-id	Configures the router ID for the router.
ip ospf admin-state	Enables or disables the administration of OSPF on the router.
ip ospf route-tag	Configures a tag value for Autonomous System External (ASE) routes created.
ip ospf spf-timer	Configures timers for SPF calculation.
ip ospf mtu-checking	Enables or disables the use of Maximum Transfer Unit (MTU) checking.
ip ospf extlsdb-limit	Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.
ip ospf exit-overflow-interval	This command sets the overflow interval value.
ip ospf default-originate	Enables or disables OSPF redistribution
ip ospf area default-metric	Creates or deletes a default metric for stub or Not So Stubby Area (NSSA) areas.
ip ospf bfd-state	Enables or disables the registration of OSPF with the BFD protocol.

MIB Objects

```
ospfGeneralGroup
   ospfRouterId
   ospfAdminStat
   ospfVersionNumber
   ospfAreaBdrRtrStatus
   ospfASBdrRtrStatus
   ospfExternLsaCount
   ospfExternLsaCksumSum
   ospfTOSSupport
   ospfOriginateNewLsas
   ospfRxNewLsas
   ospfExtLsdbLimit
   ospfExitOverflowInterval
alaProtocolospf
   alaOspfRedistRouteTag
   alaOspfTimerSpfDelay
   alaOspfTimerSpfHold
   alaOspfRouteNumber
   alaOspfMTUCheck
   alaOspfOpaqueTransitCapability
   alaOspfBfdStatus
```

show ip ospf border-routers

Displays information regarding all or specified border routers.

show ip ospf border-routers [*area_id***] [***router_id***] [***tos***] [***gateway***]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
router_id	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
tos	The Type of Service. The valid range is 0–15. Only ToS value 0 is supported at this time.
gateway	The 32-bit IP address of the gateway for the border router being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display a list of border routers known by this OSPF router.
- By using the optional parameters, you can display the border routers using the specified parameter. For example, to find a router using a router ID of 1.1.1.1, enter the command using the router ID of 1.1.1.1 as a search criteria.
- See the related commands sections below to modify the list.

Examples

```
-> show ip ospf border-routers 10.0.0.0

Router Id              Area Id            Gateway         TOS    Metric
-----------------+-----------------+--------------------+------+--------
10.0.0.0           1.0.0.1            143.209.92.71       1       1
```

output definitions

Router ID	The unique identification for the router.
Area ID	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
Gateway	The next hop interface on which the border router has been learned.
ToS	The Type of Service. Only ToS value 0 is supported at this time.
Metric	The cost to the border router.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays the OSPF status and general configuration parameters.

MIB Objects

```
alaOspfBdrRouterAreaId
alaOspfBdrRouterId
alaOspfBdrRouterTos
alaOspfBdrRouterMetric
```

show ip ospf ext-lsdb

Displays external Link State Advertisements known by this router.

show ip ospf ext-lsdb [linkstate-id *ls_id***] [router-id** *router_id***]**

Syntax Definitions

ls_id	The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.
router_id	The Router ID. The ID is a unique 32-bit value such as an IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display the external link state database (LSDB) for the OSPF router.
- This command can be used for OSPF debugging purposes, specifically to narrow down sections of attached areas to determine which sections are receiving the specified external LSAs. You may specify only the parameters from the area LSDB in which you are interested using the optional command parameters.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf ext-lsdb

      LS Id         Orig Router-Id     SeqNo      Age     Protocol
-----------------+-----------------+----------+--------+----------
  198.168.100.100    198.168.100.100      10      100     STATIC
```

output definitions

LS Id	The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.
Orig Router-Id	The router ID of the router that originated the external LSDB.
SeqNo	The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).
Age	The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.
Protocol	The type of protocol, if any.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf extlsdb-limit	Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.

MIB Objects

```
ospfExtLsdbTable
   ospfExtLsdbLsid
   ospfExtLsdbRouterId
   ospfExtLsdbSequence
   ospfExtLsdbAge
   ospfExtLsdbType
```

show ip ospf host

Displays information on the configured OSPF hosts.

show ip ospf host [*ip_address***]**

Syntax Definitions

ip_address	A 32-bit IP address for a directly attached host.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display general information for OSPF hosts directly attached to this router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf host 172.22.2.115

   Host Address     TOS     Metric     Status       AreaId
-----------------+-------+----------+--------+-----------------
 143.209.92.12       1            0      Up     0.0.0.0
```

output definitions

Host Address	A 32-bit IP address for a directly attached host. This can be set using the **ip ospf host** command.
ToS	The Type of Service traffic from the host is labeled as. ToS is set using the **ip ospf host** command.
Metric	The metric assigned to the host. Metric is set using the **ip ospf host** command.
Status	Whether the host is enabled or disabled.
AreaId	The area identification for the host's area.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf host	Creates and deletes an OSPF entry for directly attached hosts.

MIB Objects

```
ospfHostTable
   ospfHostIpAddress
   ospfHostTOS
   ospfHostMetric
   ospfHostStatus
   ospfHostAreaID
```

show ip ospf lsdb

Displays LSAs in the Link State Database associated with each area.

show ip ospf lsdb [*area_id*] **[rtr | net | netsum | asbrsum] [linkstate-id** *ls_id***] [router-id** *router_id***]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
rtr	Specifies router LSAs.
net	Specifies network LSAs.
netsum	Specifies network summary LSAs.
asbrsum	Specifies Autonomous System Border Router summary LSAs.
ls_id	The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.
router_id	The Router ID. The ID is a unique 32-bit value such as an IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display the Link State Database (LSDB) of the OSPF router. This command can be used for OSPF debugging purposes, specifically to narrow down sections of an area to determine which sections are receiving the specified link state advertisements. You may specify only the parameters from the area LSDB in which you are interested using the optional command parameters.
- You can view link state advertisements by specifying either a link state identifier or a router identifier. However, when specifying a router ID, you must also supply a valid link state ID.

Examples

```
-> show ip ospf lsdb
    Area Id       Type        LS Id        Orig Router-Id     SeqNo      Age
----------------+-------+---------------+---------------+------------+-----
0.0.0.1          OSPF   198.168.100.100  198.168.100.100     1        100
```

output definitions

Area Id	The area identification for the area to which the record belongs.
Type	The protocol type from where the route was learned.
LS Id	The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.
Orig Router-Id	The router ID of the router that originated the external LSDB.

output definitions (continued)

SeqNo	The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).
Age	The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf	Displays the OSPF status and general configuration parameters.

MIB Objects

```
ospfLsdbTable
   ospfLsdbAreaId
   ospfLsdbType
   ospfLsdbLsid
   ospfLsdbRouterId
   ospfLsdbSequence
   ospfLsdbAge
```

show ip ospf neighbor

Displays information on OSPF non-virtual neighbor routers.

show ip ospf neighbor [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address of the neighboring router.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display all non-virtual neighbors of the OSPF router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf neighbor
                                                  Domain   Domain
  IP Address        Area Id          Router Id      Name     ID      State  Type
----------------+---------------+--------------+--------+--------+-------+------
12.1.1.2         0.0.0.1          2.2.2.2         Vlan     12       Full    Dynamic
10.1.1.1         0.0.0.0          1.1.1.1         Tunnel   NA       Full    Dynamic
13.1.1.2         0.0.0.1          3.3.3.3         Service  1200     Full    Dynamic
```

output definitions

IP Address	The IP address of the neighbor.
Area Id	A unique 32-bit value, such as an IP address, that identifies the neighboring router in the Autonomous System.
Router Id	The unique identification for the neighboring router.
Domain Name	The domain on which the neighbor is reachable (**VLAN**, **Service**, or **Tunnel**).
Domain ID	The VLAN ID or service ID on which the neighbor is reachable. This field displays “NA” for IP tunnels.
State	The state of the OSPF neighbor adjacency.
Type	What type of neighbor, either **Dynamic** (learned) or **Static**.

```
-> show ip ospf neighbor 12.1.1.2
Neighbor's IP Address                = 12.1.1.2,
Neighbor's Router Id                 = 2.2.2.2,
Neighbor's Area Id                   = 0.0.0.1,
Neighbors's Domain Name             = Vlan,
Neighbors's Domain ID               = 12,
Neighbor's DR Address                = 12.1.1.2,
Neighbor's BDR Address               = 12.1.1.1,
Neighbor's Priority/Eligibility      = 1,
Neighbor's State                     = Full,
Hello Suppressed ?                   = No,
Neighbor's type                      = Dynamic,
# of State Events                    = 6,
Mode                                 = Slave,
MD5 Sequence Number                  = 0,
Time since Last Hello                = 7 sec,
# of Outstanding LS Requests         = 0,
# of Outstanding LS Acknowledgements = 0,
# of Outstanding LS Retransmissions  = 0,
Restart Helper Status                = notHelping,
Restart Age (in seconds)             = 0 sec,
Last Restart Helper Exit Reason      = None
Opaque LSA Capability                = Yes

-> show ip ospf neighbor 13.1.1.2
Neighbor's IP Address                = 14.1.1.2,
Neighbor's Router Id                 = 3.3.3.3,
Neighbor's Area Id                   = 0.0.0.1,
Neighbors's Domain Name              = Service,
Neighbors's Domain ID                = 1200,
Neighbor's DR Address                = 13.1.1.2,
Neighbor's BDR Address               = 13.1.1.1,
Neighbor's Priority/Eligibility      = 1,
Neighbor's State                     = Full,
Hello Suppressed ?                   = No,
Neighbor's type                      = Dynamic,
# of State Events                    = 6,
Mode                                 = Slave,
MD5 Sequence Number                  = 0,
Time since Last Hello                = 7 sec,
# of Outstanding LS Requests         = 0,
# of Outstanding LS Acknowledgements = 0,
# of Outstanding LS Retransmissions  = 0,
Restart Helper Status                = notHelping,
Restart Age (in seconds)             = 0 sec,
Last Restart Helper Exit Reason      = None
Opaque LSA Capability                = Yes

-> show ip ospf neighbor 10.1.1.1
Neighbor's IP Address                = 10.1.1.1,
Neighbor's Router Id                 = 1.1.1.1,
Neighbor's Area Id                   = 0.0.0.0,
Neighbors's Domain Name              = Tunnel,
Neighbors's Domain ID                = NA,
Neighbor's DR Address                = 10.1.1.1,
Neighbor's BDR Address               = 0.0.0.0,
Neighbor's Priority/Eligibility      = 1,
Neighbor's State                     = Full,
Hello Suppressed ?                   = No,
```

```
Neighbor's type                     = Dynamic,
# of State Events                   = 6,
Mode                                = Master,
MD5 Sequence Number                 = 0,
Time since Last Hello               = 7 sec,
# of Outstanding LS Requests        = 0,
# of Outstanding LS Acknowledgements = 0,
# of Outstanding LS Retransmissions  = 0,
Restart Helper Status               = notHelping,
Restart Age (in seconds)            = 0 sec,
Last Restart Helper Exit Reason     = None
Opaque LSA Capability               = Yes
```

output definitions

Neighbor's IP Address	The IP address of the neighbor.
Neighbor's Router Id	The identification number for the selected host's record. It is most often the router's IP address.
Neighbor's Area Id	Identifier of the OSPF Area to which the neighbor is attached. 255.255.255.255 shows that this neighbor is not attached to any area.
Neighbor's Domain Name	The domain on which the neighbor is reachable (**VLAN**, **Service**, or **Tunnel**).
Neighbor's Domain ID	The VLAN ID or service ID on which the neighbor is reachable. This field displays "NA" for IP tunnels.
Neighbor's DR Address	The address of the neighbors Designated Router.
Neighbor's BDR Address	The address of the neighbors Backup Designated Router.
Neighbor's Priority	The priority value for this neighbor becoming the DR.
Neighbor's State	The condition of the OSPF neighbor's state machine.
Hello Suppressed	Whether sending hello messages to this neighbor is suppressed.
Neighbor's type	What type of neighbor this is, either **dynamic** or **static**.
DR Eligible	Shows the eligibility status of the static neighbor. If it is configured as "ineligible" during creation of the neighbor, it shows up as **No**. Otherwise, if configured as Eligible (the default), it shows up as **Yes**.
# of State Events	The number of state events restricted for this neighbor and the local router.
Mode	The role the neighbor has with the local router during DD Exchange, which can be Master or Slave.
MD5 Sequence Number	The sequence number of the MD5 authorization key.
Time since Last Hello	The amount of time (in seconds) since the last HELLO messages was received from this neighbor.
# of Outstanding LS Requests	The number of Link State requests to this neighbor that have not received a response from this neighbor.
# of Outstanding LS Acknowledgements	Number of Link state Acknowledgements queued up by the local router to be sent to the neighbor.
# of Outstanding LS Retransmissions	The number of Link State updates to the neighbor that need to be retransmitted by the OSPF router.

output definitions (continued)

Restart Helper Status	Indicates whether the router is acting as a hitless restart helper for the neighbor.
Restart Age	The remaining time, in seconds, for the current OSPF hitless restart interval if the router is acting as a restart helper for the neighbor.
Last Restart Helper Exit Reason	The outcome of the last attempt at acting as a hitless restart helper for the neighbor.
Opaque LSA Capability	Whether the opaque LSA accept and retransmit capability for OSPF is enabled or disabled.

Release History

Release 7.1.1; command was introduced.
Release 8.6R1; “Domain Name”, “Domain ID”, “Neighbor’s Domain Name”, and “Neighbor’s Domain ID” fields added.

Related Commands

ip ospf neighbor	Creates a static neighbor on a Non Broadcast Multi Access (NBMA) interface.

MIB Objects

```
ospfNbrTable
   ospfNbrIpAddr
   ospfNbrRtrId
   ospfNbrOptions
   ospfNbrPriority
   ospfNbrState
   ospfNbrEvents
   ospfNbrHelloSuppressed
alaOspfNbrAugTable
   alaOspfNbrRestartHelperStatus
   alaOspfNbrRestartHelperAge
   alaOspfNbrRestartHelperExitReason
   alaOspfNbrAreaId
   alaOspfNbrDrAddress
   alaOspfNbrBdrAddress
   alaOspfNbrType
   alaOspfNbrMode
   alaOspfNbrMd5SeqNo
   alaOspfNbrLastHello
   alaOspfNbrPendingLSreq
   alaOspfNbrPendingLSack
   alaOspfNbrPendingLSupd
   alaOspfNbrIfIndex
```

show ip ospf routes

Displays the OSPF routes known to the router.

show ip ospf routes [*ip_address mask tos gateway***]**

Syntax Definitions

ip_address	A 32-bit IP address of the route destination in dotted decimal format.
mask	The IP subnet mask of the route destination.
tos	The Type of Service of the route.
gateway	The next hop IP address for this router.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If no variables are entered, all routes are displayed. If the variables are entered, then only routes matching the specified criteria are shown. All the variables described above must be entered for a route match. If all of the variables are not entered, an error message is returned.

Examples

```
-> show ip ospf routes
                                                Domain  Domain
 Destination/Mask          Gateway       Metric   Name     ID          Type
--------------------+-----------------+--------+--------+--------+----------
2.2.2.2/32           12.1.1.2          1        Vlan     12        Intra
12.1.1.0/24          12.1.1.1          1        Vlan     12        Intra
10.1.1.0/24          10.1.1.2          1        Tunnel   NA       Intra
20.1.1.0/24          120.1.1.2         2        Service  120       Inter
172.28.4.0/24        120.1.1.2         2        Service  120       Inter
198.168.100.100      195.5.2.8         0        Vlan     5         AS-Ext
```

output definitions

Destination/Mask	The destination address of the route. This can also display the destination IP address mask if it is known.
Gateway	The gateway address of the route.
Metric	The cost of the route.
Domain Name	The domain on which the gateway can be routed (**VLAN**, **Service**, or **Tunnel**).
Domain ID	The VLAN ID or service ID on which the gateway can be routed. This field displays “NA” for IP tunnels.
Type	The type of OSPF route.

Release History

Release 7.1.1; command was introduced.
Release 8.6R2; “Domain Name” and “Domain ID” fields added.

Related Commands

show ip ospf	Displays the OSPF status and general configuration parameters.

MIB Objects

```
alaOspfRouteTable
   alaOspfRouteDest
   alaOspfRouteMask
   alaOspfRouteNextHop
   alaOspfRouteIfIndex
   alaOspfRouteType
   alaOspfRouteMetric1
```

show ip ospf virtual-link

Displays virtual link information. A virtual link is used to connect OSPF backbone routers that are not physically contiguous.

show ip ospf virtual-link [*router_id***]**

Syntax Definitions

router_id	The router ID of the remote end of the virtual link that is to be viewed.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf virtual-link
                                        State
 Transit AreaId      Router-id    Link / Adjacency  AuthType   OperStatus
----------------+----------------+----------------+----------+------------
1.1.1.1           172.17.1.1     P2P  / Full       none        up
```

output definitions

Transit AreaId	The area identification for the area assigned to the virtual link.
Router-Id	The destination router identification for the virtual link.
State Link	The state of the virtual link with regards to the local router.
State Adjacency	The state of the virtual link adjacency.
AuthType	The type of authorization employed by the virtual link.
OperStatus	Displays whether the virtual link is enabled or disabled.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf virtual-link	Creates or deletes a virtual link.
show ip ospf virtual-neighbor	Displays OSPF virtual neighbors.

MIB Objects

```
ospfVirtIfTable
   ospfVirtIfAreaId
   ospfVirtIfNeighbor
   ospfVirtIfState
   ospfVirtIfAuthType
```

show ip ospf virtual-neighbor

Displays OSPF virtual neighbors. A virtual neighbor is connected to the router through a virtual link rather than a physical one.

show ip ospf virtual-neighbor *area_id router_id*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
router_id	The router ID of the remote end of the virtual link that is to be viewed.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display all virtual neighbors for the OSPF router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf virtual-neighbor 0.0.0.0 10.0.0.1

     AreaId           RouterId     Priority Events RxmtQLen LastHello  State
-----------------+----------------+--------+------+--------+---------+-------
 0.0.0.0           10.0.0.0           1        10     100      323     INIT
```

output definitions

AreaId	The area identification for the area of which the virtual neighbor is a part.
RouterId	The router identification of the virtual neighbor.
Priority	The number used to determine whether the virtual neighbor will become the designated router for its area.
Events	The number of OSPF control message sent by the neighbor to the router.
RxmtQlen	The length (in number of packets) of the retransmit queue.
LastHello	The last Hello message sent by the neighbor
State	The current state the virtual neighbor is in relative to the router; this will be INIT, Exchange, or Full.

```
-> show ip ospf virtual-neighbor 0.0.0.1 2.0.0.254
Neighbor's IP Address               = 2.0.0.254,
Neighbor's Router Id                = 2.0.0.254,
Neighbor's Area Id                  = 0.0.0.1,
Neighbor's DR Address               = 2.0.0.1,
Neighbor's BDR Address              = 2.0.0.254,
Neighbor's Priority                 = 1,
Neighbor's State                    = Full,
Hello Suppressed ?                  = No,
Neighbor's type                     = Dynamic,
# of State Events                   = 6,
Mode = Master,
MD5 Sequence Number                 = 0,
Time since Last Hello               = 5 sec,
Last DD I_M_MS                      =
# of Outstanding LS Requests        = 0,
# of Outstanding LS Acknowledgements= 0,
# of Outstanding LS Retransmissions = 0,
Restart Helper Status               = Not Restarting,
Restart Age (in seconds)            = 0 sec,
Last Restart Helper Exit Reason     = None
```

output definitions

Neighbor's IP Address	The IP address of the virtual neighbor.
Neighbor's Router Id	The identification number for the selected host's record. It is most often the router's IP address.
Neighbor's Area Id	Identifier of the OSPF Area to which the virtual neighbor is attached. 255.255.255.255 shows that this virtual neighbor is not attached to any area.
Neighbor's DR Address	The address of the virtual neighbor's Designated Router.
Neighbor's BDR Address	The address of the virtual neighbor's Backup Designated Router.
Neighbor's Priority	The priority value for this virtual neighbor becoming the DR.
Neighbor's State	The condition of the OSPF virtual neighbor's state machine.
Hello Suppressed	Whether sending hello messages to this virtual neighbor is suppressed.
Neighbor's type	What type of virtual neighbor this is, either dynamic or static.
DR Eligible	Shows the eligibility status of the virtual neighbor. If it is configured as "ineligible" during creation of the neighbor, it shows up as **No**. Otherwise, if configured as Eligible (the default), it shows up as **Yes**.
# of State Events	The number of state events restricted for this virtual neighbor and the local router.
Mode	The role the virtual neighbor has with the local router during DD Exchange, which can be Master or Slave.
MD5 Sequence Number	The sequence number of the MD5 authorization key.
Time since Last Hello	The amount of time (in seconds) since the last HELLO messages was received from this virtual neighbor.
Last DD I_M_MS	The initialize (I), more (M) and master (MS) bits, and Options field Data Description (DD) packet received from the virtual neighbor. This parameter is used to determine whether the next DD packet has been received or not.

output definitions (continued)

# of Outstanding LS Requests	The number of Link State requests to this virtual neighbor that have not received a response from this virtual neighbor.
# of Outstanding LS Acknowledgements	Number of Link state Acknowledgements queued up by the local router to be sent to the virtual neighbor.
# of Outstanding LS Retransmissions	The number of Link State updates to the virtual neighbor that need to be retransmitted by the OSPF router.
Restart Helper Status	Indicates whether the router is acting as a hitless restart helper for the virtual neighbor.
Restart Age	The remaining time, in seconds, for the current OSPF hitless restart interval if the router is acting as a restart helper for the virtual neighbor.
Last Restart Helper Exit Reason	The outcome of the last attempt at acting as a hitless restart helper for the virtual neighbor.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf virtual-link	Creates or deletes a virtual link.

MIB Objects

```
ospfVirtNbrTable
   ospfVirtNbrArea
   ospfVirtNbrRtrId
   ospfVirtNbrState
alaOspfVirtNbrAugTable
   alaOspfVirtNbrRestartHelperStatus
   alaOspfVirtNbrRestartHelperAge
   alaOspfVirtNbrRestartHelperExitReason
```

show ip ospf area

Displays either all OSPF areas, or a specified OSPF area.

show ip ospf area [*area_id*]

Syntax Definitions

area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Allows you to view the details of a specified OSPF area.
- Not specifying an OSPF area will display all known areas for the OSPF router.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ip ospf area

    Area Id      AdminStatus      Type       OperStatus
---------------+-------------+-------------+------------
1.1.1.1           disabled     normal       down
0.0.0.1           disabled     normal       down

-> show ip ospf area 0.0.0.0

Area Identifier                          = 1.1.1.1,
Admin Status                             = Disabled,
Operational Status                       = Down,
Area Type                                = normal,
Area Summary                             = Enabled,
Time since last SPF Run                  = 00h:00m:27s,
# of Area Border Routers known           = 0,
# of AS Border Routers known             = 0,
# of LSAs in area                        = 0,
# of SPF Calculations done               = 0,
# of Incremental SPF Calculations done   = 0,
# of Neighbors in Init State             = 0,
# of Neighbors in 2-Way State            = 0,
# of Neighbors in Exchange State         = 0,
# of Neighbors in Full State             = 0,
# of Interfaces attached                 = 0
Attached Interfaces                      = vlan-213
```

output definitions

Area Identifier	The unique 32-bit value, such as IP address, that identifies the OSPF area in the AS.
Admin Status	Whether the area is enabled or disabled.
Operational Status	Whether the area is active.
Area Type	The area type. This field will be **normal**, **stub**, or **NSSA**.
Area Summary	Whether Area Summary is enabled or disabled.
Time since last SPF Run	The last time the Shortest Path First calculation was performed.
# of Area Border Routers known	The number of Area Border Routers in the area.
# of AS Border Routers known	The number of Autonomous System Border Routers in the area.
# of LSAs	The total number of Link State Advertisements for the Area.
# of SPF Calculations	The number of times the area has calculated the Shortest Path.
# of Incremental SPF Calculations	The number of incremental Shortest Path First calculations that have been performed in the area.
# of Neighbors in Init State	The number of OSPF neighbors that are in initialization.
# of Neighbors in 2-Way State	The number of OSPF 2-way state neighbors in this area.
# of Neighbors in Exchange State	The number of OSPF neighbors that are currently establishing their status.
# of Neighbors in Full State	The number of OSPF neighbors.
# of Interfaces attached	The number of OSPF interfaces.
Attached Interfaces	The names of the OSPF interfaces attached to this area.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area, assigning default metric, cost, and type.
ip ospf area range	Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
show ip ospf interface	Displays OSPF interface information.

MIB Objects

```
ospfAreaTable
   ospfAreaId
   ospfImportAsExtern
   ospfSpfRuns
   ospfAreaBdrRtrCount
   ospfAsBdrRtrCount
   ospfAreaLsaCount
   ospfAreaSummary
   ospfAreaStatus
alaOspfIfAugTable
   alaOspfIfIntfName
```

show ip ospf area range

Displays all or specified route summaries in a given area.

show ip ospf area *area_id* **range [{summary | nssa}** *ip_address ip_mask***]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
summary	Specifies that routes are summarized.
nssa	Specifies the Not So Stubby Area (NSSA) routers are summarized. *This parameter is not supported on an OmniSwitch 6560.*
ip_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Allows you to view the details of a specified OSPF area range.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ip ospf area 0.0.0.0 range

     AreaId        Type     Destination        Advertise
---------------+---------+-----------------+-----------
0.0.0.0          Summary   192.168.12.1/24   Matching
0.0.0.0          NSSA      143.209.92.71/24  noMatching
```

output definitions

AreaId	The area identification for the area range.
Type	The type of area the range is associated with.
Destination	The destination address of the range.
Advertise	Shows the filter effect of the range. LSAs in the range are either advertised (Matching) or not advertised (noMatching).

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area range	Creates a route summarization instance whereby a range of addresses assigned for the route at the area border router will be advertised.

MIB Objects

```
ospfAreaRangeTable
   ospfAreaRangeAreaId
   ospfAreaRangeNet
   ospfAreaRangeMask
   ospfAreaRangeStatus
   ospfAreaRangeEffect
```

show ip ospf area stub

Displays stub default area metrics, if configured.

show ip ospf area *area_id* **stub**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip ospf area 0.0.0.1 stub

    Area Id       TOS     Metric    MetricType
---------------+-------+----------+------------
0.0.0.1           1          1        ospf
```

output definitions

Area Id	The identification number of the stub area.
TOS	The Type of Service assignment.
Metric	The metric assignment of the default router in the stub area.
MetricType	The metric type of the stub area. It will be either **ospf**, **type1**, or **type2**.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area.

MIB Objects

```
ospfStubAreaTable
   ospfStubAreaId
   ospfStubTOS
   ospfStubMetric
   ospfStubStatus
   ospfStubMetricType
```

show ip ospf interface

Displays OSPF interface information.

show ip ospf interface [*interface_name***]**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Not specifying an interface name displays all known interfaces for the OSPF router.

Examples

No interface name is specified:

```
-> show ip ospf interface
    Interface           DR           Backup DR      Admin    Oper           BFD
      Name           Address         Address       Status   Status  State  Status
------------------+--------------+--------------+--------+------+-------+--------
vlan-213          100.10.10.88    100.10.10.2     enabled  up     BDR     disabled
vlan-215          101.10.10.2     0.0.0.0         enabled  up     DR      enabled
vlan-220          10.10.20.1      0.0.0.0         enabled  up     DR      disabled
service-1200      13.1.1.1        13.1.1.2        enabled  UP     BDR     enabled
tunnel-1          10.1.1.2        0.0.0.0         enabled  UP     DR      enabled
```

output definitions

Interface Name	The name of the interface.
DR Address	The designated router IP address on this network segment.
Backup DR Address	The IP address of the backup designated router.
Admin Status	The current administration status of the interface, either **enabled** or **disabled**.
Oper Status	Whether the interface is an active OSPF interface.
State	The current state of the OSPF interface. It will be **down**, **up**, **dp**, **dr**, or **other**.
BFD Status	The current status of BFD for the OSPF interface.

The following is an example of MD5 authentication (an interface name is used in this example).

```
-> show ip ospf interface vlan-213
Interface IP Name                    = vlan-213
Interface IP Address                 = 100.10.10.2,
```

```
Interface IP Mask                     = 255.255.255.0,
Domain Name                           = Vlan,
Domain ID                             = 213,
Admin Status                          = Enabled,
Operational Status                    = Up,
OSPF Interface State                  = BDR,
Interface Type                        = Broadcast,
Area Id                               = 0.0.0.2,
Designated Router IP Address          = 100.10.10.88,
Designated Router RouterId            = 100.10.10.88,
Backup Designated Router IP Address   = 100.10.10.2,
Backup Designated Router RouterId     = 192.169.1.2,
MTU  (bytes)                          = 1500,
Metric Cost                           = 1,
Priority                              = 1,
Hello Interval (seconds)              = 10,
Transit Delay (seconds)               = 1,
Retrans Interval (seconds)            = 5,
Dead Interval (seconds)               = 40,
Poll Interval (seconds)               = 120,
Link Type                             = Broadcast,
Authentication Type                   = md5,
# of Events                           = 2,
# of Init State Neighbors             = 0,
# of 2-Way State Neighbors            = 0,
# of Exchange State Neighbors         = 0,
# of Full State Neighbors             = 1
BFD status                            = Disabled,
DR-Only Option for BFD                = Disabled
```

The following is an example of simple authentication (an interface name is used in this example):

```
-> show ip ospf interface vlan-215
Interface IP Name                     = vlan-215
Interface IP Address                  = 101.10.10.2,
Interface IP Mask                     = 255.255.255.0,
Domain Name                           = Vlan,
Domain ID                             = 215,
Admin Status                          = Enabled,
Operational Status                    = Up,
OSPF Interface State                  = DR,
Interface Type                        = Broadcast,
Area Id                               = 0.0.0.2,
Designated Router IP Address          = 101.10.10.2,
Designated Router RouterId            = 192.169.1.2,
Backup Designated Router IP Address   = 0.0.0.0,
Backup Designated Router RouterId     = 0.0.0.0,
MTU  (bytes)                          = 1500,
Metric Cost                           = 1,
Priority                              = 1,
Hello Interval (seconds)              = 10,
Transit Delay (seconds)               = 1,
Retrans Interval (seconds)            = 5,
Dead Interval (seconds)               = 40,
Poll Interval (seconds)               = 120,
Link Type                             = Broadcast,
Authentication Type                   = simple,
Authentication Key                    = Set,
# of Events                           = 3,
```

```
# of Init State Neighbors             = 0,
# of Exchange State Neighbors         = 0,
# of 2-Way State Neighbors            = 0,
# of Full State Neighbors             = 0
BFD Status                            = Disabled,
DR-Only Option for BFD                = Disabled
```

The following is an example of keychain authentication (an interface name is used in this example):

```
-> show ip ospf interface vlan-220
Interface IP Name                     = vlan-220,
Interface IP Address                  = 10.10.20.1,
Interface IP Mask                     = 255.255.255.0,
Domain Name                           = Vlan,
Domain ID                             = 220,
Admin Status                          = Enabled,
Operational Status                    = Up,
OSPF Interface State                  = DR,
Interface Type                        = Broadcast,
Area Id                               = 0.0.0.0,
Designated Router IP Address          = 10.10.20.1,
Designated Router RouterId            = 10.10.10.1,
Backup Designated Router IP Address   = 0.0.0.0,
Backup Designated Router RouterId     = 0.0.0.0,
MTU  (bytes)                          = 1500,
Metric Cost                           = 1,
Priority                              = 1,
Hello Interval (seconds)              = 10,
Transit Delay (seconds)               = 1,
Retrans Interval (seconds)            = 5,
Dead Interval (seconds)               = 40,
Poll Interval (seconds)               = 120,
Link Type                             = Broadcast,
Authentication Type                   = Keychain(1),
# of Events                           = 2,
# of Init State Neighbors             = 0,
# of 2-Way State Neighbors            = 0,
# of Exchange State Neighbors         = 0,
# of Full State Neighbors             = 0,
# of type-9 LSAs on this interface    = 0,
BFD status                            = Disabled,
DR-Only Option for BFD                = Disabled
```

The following are examples of an OSPF interface configured for an IP interface that is bound to a service and configured for an IP interface that is bound to a tunnel (an interface name is used in each example):

```
-> show ip ospf interface service-1200
Interface IP Name                     = service-1200,
Interface IP Address                  = 13.1.1.2,
Interface IP Mask                     = 255.255.255.0,
Domain Name                           = Service,
Domain ID                             = 1200,
Admin Status                          = Enabled,
Operational Status                    = Up,
OSPF Interface State                  = BDR,
Interface Type                        = Broadcast,
Area Id                               = 0.0.0.1,
Designated Router IP Address          = 13.1.1.1,
Designated Router RouterId            = 172.28.4.133,
Backup Designated Router IP Address   = 13.1.1.2,
```

```
Backup Designated Router RouterId     = 2.2.2.2,
MTU  (bytes)                          = 1500,
Metric Cost                           = 1,
Priority                              = 1,
Hello Interval (seconds)              = 10,
Transit Delay (seconds)               = 1,
Retrans Interval (seconds)            = 5,
Dead Interval (seconds)               = 40,
Poll Interval (seconds)               = 120,
Link Type                             = Broadcast,
Authentication Type                   = none,
# of Events                           = 3,
# of Init State Neighbors             = 0,
# of 2-Way State Neighbors            = 0,
# of Exchange State Neighbors         = 0,
# of Full State Neighbors             = 1,
# of type-9 LSAs on this interface    = 0,
BFD status                            = Enabled,
DR-Only Option for BFD                = Disabled

-> show ip ospf interface tunnel-1
Interface IP Name                     = tunnel-1,
Interface IP Address                  = 10.1.1.2,
Interface IP Mask                     = 255.255.255.0,
Domain Name                           = Tunnel,
Domain ID                             = NA,
Admin Status                          = Enabled,
Operational Status                    = Up,
OSPF Interface State                  = DR,
Interface Type                        = Broadcast,
Area Id                               = 0.0.0.0,
Designated Router IP Address          = 10.1.1.2,
Designated Router RouterId            = 20.1.1.1,
Backup Designated Router IP Address   = 0.0.0.0,
Backup Designated Router RouterId     = 0.0.0.0,
MTU  (bytes)                          = 1480,
Metric Cost                           = 1,
Priority                              = 1,
Hello Interval (seconds)              = 10,
Transit Delay (seconds)               = 1,
Retrans Interval (seconds)            = 5,
Dead Interval (seconds)               = 40,
Poll Interval (seconds)               = 120,
Link Type                             = Broadcast,
Authentication Type                   = none,
# of Events                           = 3,
# of Init State Neighbors             = 0,
# of 2-Way State Neighbors            = 0,
# of Exchange State Neighbors         = 0,
# of Full State Neighbors             = 0,
# of type-9 LSAs on this interface    = 0,
BFD status                            = Enabled,
DR-Only Option for BFD                = Disabled
```

Output fields when an interface name is specified are described below:

output definitions

Interface IP Name	The name of the IP interface on which OSPF is configured.
Interface IP Address	The IP address assigned to the interface.
Interface IP Mask	The IP mask associated with the IP address assigned to the interface.
Domain Name	The domain on which the IP interface was configured (**VLAN**, **Service**, or **Tunnel**).
Domain ID	The VLAN ID or service ID on which the IP interface was configured. This field displays "NA" for IP tunnels.
Admin Status	The current administration status of the interface (**enabled** or **disabled**).
Operational Status	Whether the interface is an active OSPF interface.
OSPF Interface State	The current state of the OSPF interface (**down**, **up**, **dp**, **dr**, or **other**).
Interface Type	The OSPF interface type, which can be Broadcast, NBMA, Point-to-Point, or Point-to-Multipoint.
Area Id	The area identification number to which the interface is assigned. This field is not applicable if an interface has not yet been assigned to an area.
Designated Router IP Address	The designated router IP address.
Designated Router RouterId	The identification number of the designated router.
Backup Designated Router IP Address	The IP address of the backup designated router.
Backup Designated Router RouterId	The identification number of the backup designated router.
MTU	The Maximum Transfer Unit (in bytes) for the interface.
Metric Cost	The cost added to routes learned on this interface.
Priority	The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.
Hello Interval	The number of seconds between hello messages sent out on the interface.
Transit Delay	The estimated number of seconds required to transmit a link state update over this interface.
Retrans Interval	The number of seconds the interface waits before resending hello messages.
Dead Interval	The number of seconds the interface waits for hello messages received from a neighbor before declaring the neighbor as dead.
Poll Interval	The larger time interval, in seconds, between hello messages sent to inactive neighbors.
Link Type	The IP interface type (**broadcast** or **non broadcast**).
Authentication Type	The type of authentication used by this interface (**None**, **Simple**, **MD5**, or **Keychain**).
#	The indexing of the MD5 key. (This field is only displayed for MD5 authentication.)

output definitions (continued)

Id	A key identifier that identifies the algorithm and MD5 secret key associated with this interface. (This field is only displayed for MD5 authentication.)
Key	Indicates whether the MD5 key has been set or not. (This field is only displayed for MD5 authentication.)
Status	The status of the configured MD5 authentication key. (This field is only displayed for MD5 authentication.)
StartAccept	The time that the OSPF router will start accepting packets that have been created with this key. (This field is only displayed for MD5 authentication.)
StopAccept	The time that the OSPF router will stop accepting packets that have been created with this key. (This field is only displayed for MD5 authentication.)
StartGen	The time that the OSPF router will start using this key for packet generation. (This field is only displayed for MD5 authentication.)
StopGen	The time that the OSPF router will stop using this key for packet generation. (This field is only displayed for MD5 authentication.)
Authentication Key	This field displays whether the authentication key has been configured or not. (This field is only displayed for simple and no authentication.)
# of Events	The number of interface state machine events.
# of Init State Neighbors	The number of OSPF neighbors in the initialization state.
# of 2-Way State Neighbors	The number of OSPF 2-way state neighbors on this interface.
# of Exchange State Neighbors	The number of OSPF neighbors in the exchange state.
# of Full State Neighbors	The number of OSPF neighbors in the full state. The full state is a neighbor that is recognized and passing data between itself and the interface.
# of type-9 LSAs on this interface	Number of type-9 LSA on this interface. (This field is only displayed for keychain authentication.)
BFD Status	The status of BFD on this interface.
DR-Only Option for BFD	The BFD setting for this interface. If DR-Only only is disabled then the setting is All Neighbors.

Release History

Release 7.1.1; command was introduced.
Release 8.6R2; “Domain Name” and “Domain ID” fields added.

Related Commands

ip ospf interface	Creates and deletes an OSPF interface.
ip ospf interface auth-key	Configures an OSPF authentication key for simple authentication on an interface.
ip ospf interface dead-interval	Configures the OSPF interface dead interval.
ip ospf interface hello-interval	Configures the OSPF interface hello interval.

ip ospf interface md5	Creates and deletes the OSPF interface MD5 key identification number.
ip ospf interface md5 key	Configures the OSPF key string.
ip ospf interface cost	Configures the OSPF interface cost.
ip ospf interface poll-interval	Configures the OSPF poll interval for a Non Broadcast Multi Access (NBMA) interface.
ip ospf interface priority	Configures the OSPF interface priority.
ip ospf interface retrans-interval	Configures the OSPF interface retransmit interval.
ip ospf interface transit-delay	Configures the OSPF interface transit delay.
ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface area	Configures an OSPF interface area.
ip ospf interface type	Configures the OSPF interface type.
ip ospf interface admin-state	Enables or disables the administration status on an OSPF interface.
ip ospf interface bfd-state	Enables or disables the status of BFD for an OSPF interface.
ip ospf interface bfd-state drs-only	Configures whether BFD sessions are only established with neighbors that are in the full state.

MIB Objects

```
ospfIfTable
   ospfIfIpAddress
   ospfIfAreaId
   ospfIfType
   ospfIfAdminStat
   ospfIfRtrPriority
   ospfIfTransitDelay
   ospfIfRetransInterval
   ospfIfHelloInterval
   ospfIfRtrDeadInterval
   ospfIfPollInterval
   ospfIfState
   ospfIfDesignatedRouter
   ospfIfBackupDesignatedRouter
   ospfIfEvents
   ospfIfAuthType
   ospfIfStatus
   ospfIfAuthKey
alaOspfIfMd5Table
   alaOspfIfMd5IpAddress
   alaOspfIfMd5KeyId
   alaOspfIfMd5Key
   alaOspfIfMd5EncryptKey
   alaOspfIfMd5KeyStartAccept
   alaOspfIfMd5KeyStopAccept
   alaOspfIfMd5KeyStartGenerate
   alaOspfIfMd5KeyStopGenerate
alaOspfIfAugTable
   alaOspfIfEncryptKey
   alaOspfIfIpMask
```

```
alaOspfIfDrRouterid
alaOspfIfBdrRouterid
alaOspfIfMTU
alaOspfIfInitNbrs
alaOspfIfExchNbrs
alaOspfIfFullNbrs
alaOspfIfLinkType
alaOspfIfOperStatus
alaOspfIfIntfName
alaOspfIf2WayNbrs
alaOspfIfBfdStatus
alaOspfIfBfdDrsOnly
alaOspfIfKeyChainId
alaOspfIfIfIndex
```

show ip ospf interface auth-info

Displays authentication information for the interface.

show ip ospf interface auth-info [*interface_name***]**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Not specifying an interface name displays all known interfaces for the OSPF router.
- When keychain authentication type is used for the interface, only the keychain ID is displayed. To view the keys associated with the keychain, use the keychain commands. For more information keychain management commands, refer to the “Chassis Management and Monitoring Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.

Examples

```
-> show ip ospf interface auth-info
Interface Name        Key-chain    KeyId     Key       Status        AuthMode
--------------------+------------+------+----------+------------+----------------
vlan-30-int             1           --       --       Enabled       keychain
vlan-20-int             --          10       Set      Enabled       Keyed-MD5
```

output definitions

Interface Name	The name of the interface.
Key-chain	The keychain associated with the interface.
KeyId	A key identifier that identifies the algorithm and MD5 secret key associated with this interface. (This field is only displayed for MD5 authentication.)
Key	Indicates whether the key has been set or not.
Status	The current administration status of the interface, either **enabled** or **disabled**.
AuthMode	The type of authentication used by this interface.

Release History

Release 8.4.1; command introduced.

Related Commands

ip ospf interface auth-type	Sets the OSPF interface authentication type. Authentication allows the router to only respond to other routers that have the correct authentication information.

MIB Objects

N/A

show ip ospf restart

Displays the OSPF graceful restart related configuration and status.

show ip ospf restart

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration.

Examples

```
-> show ip ospf restart
Restart Support                     = Enabled,
Restart Interval (in seconds)       = 120,
Restart Status                      = Not Restarting,
Restart Age (in seconds)            = 0,
Last Restart Exit Reason            = None,
Restart Helper Support              = Enabled,
Restart Helper Strict Checking      = Enabled,
Restart Helper Mode                 = NotHelping
```

output definitions

Restart Support	The administrative status of OSPF graceful restart, which can be **Enabled** or **Disabled**.
Restart Interval	The configured OSPF hitless restart timeout interval, in seconds. Use the **ip ospf restart-interval** command to modify this parameter.
Restart Status	The current status of OSPF graceful restart, which can be **Not Restarting**, **Unplanned Restart** (after a CMM takeover), or **Planned Restart** (before CMM takeover).
Restart Age	The remaining time, in seconds, for the current OSPF graceful restart interval.
Last Restart Exit Reason	The outcome of the last attempt at a graceful restart. If the value is **None**, then no restart has yet been attempted. If the value is **In Progress**, then a restart attempt is currently underway. Other possible values include **Completed** (successfully completed), **Timed Out** (timed out), and **Topology Changed** (aborted due to topology change).

output definitions (continued)

Restart Helper Support	The administrative status of the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart, which can be **Enabled** or **Disabled**. Use the **ip ospf restart-helper admin-state** command to modify this parameter.
Restart Helper Strict Checking	The administrative status of whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router, which can be **Enabled** or **Disabled**. Use the **ip ospf restart-helper strict-lsa-checking admin-state** command to modify this parameter.
Restart Helper Mode	Whether this OSPF router is operating as a helper to a restarting router.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf restart-support	Configures support for the graceful restart feature on an OSPF router.
ip ospf restart initiate	Initiates a planned graceful restart.

MIB Objects

N/A

27 OSPFv3 Commands

Open Shortest Path First version 3 (OSPFv3) routing is a shortest path first (SPF) or link-state protocol. This protocol is compatible with 128-bit IPv6 address space, while OSPF is compatible with 32-bit IPv4 address space. OSPFv3 is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPFv3 chooses the least-cost path as the best path.

Each participating router distributes its local state (i.e., the router's usable interfaces and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. This database is built from the collected link state advertisements of all routers. Each multi-access network that has at least two attached routers has a designated router and a backup designated router. The designated router floods a link state advertisement for the multi-access network and has other special responsibilities.

OSPFv3 allows collections of contiguous networks and hosts to be grouped together. A group, together with the routers having interfaces to any one of the included networks, is called an *are*a. Each area runs a separate copy of the basic link-state routing algorithm. This means that each area has its own topological database, as explained in the previous section.

The OmniSwitch version of OSPFv3 complies with RFCs 2740, 1826, 1827, 2553, 2373, 2374, and 2460.

MIB information for OSPFv3 is as follows:

Filename: ALCATEL-IND1-VIRTUALROUTER-MIB.mib
Module: alcatelIND1VirtualRouterMIB

Filename: ALCATEL-IND1-OSPF3-MIB.mib
Module: alcatelIND1OSPF3MIB

Filename: OSPFV3-MIB.mib
Module: ospfv3MIB

The following is a list of the commands for configuring OSPFv3:

Global OSPFv3 Commands	**ipv6 load ospf** **ipv6 ospf admin-state** **ipv6 ospf host** **ipv6 ospf mtu-checking** **ipv6 ospf route-tag** **ipv6 ospf spf-timer** **ipv6 ospf virtual-link** **show ipv6 ospf** **show ipv6 ospf border-routers** **show ipv6 ospf host** **show ipv6 ospf lsdb** **show ipv6 ospf neighbor** **show ipv6 ospf routes** **show ipv6 ospf virtual-link**
OSPFv3 Area Commands	**ipv6 ospf area** **ipv6 ospf area area-summary** **ipv6 ospf area nssa-translator-role** **ipv6 ospf area nssa-translator-stab-interval** **ipv6 ospf area nssa-summarize** **show ipv6 ospf area**
OSPFv3 Interface Commands	**ipv6 ospf interface** **ipv6 ospf interface admin-state** **ipv6 ospf interface suppress-link-lsa** **ipv6 ospf interface type** **ipv6 ospf neighbor** **ipv6 ospf interface area** **ipv6 ospf interface dead-interval** **ipv6 ospf interface hello-interval** **ipv6 ospf interface cost** **ipv6 ospf interface priority** **ipv6 ospf interface retrans-interval** **ipv6 ospf interface transit-delay** **show ipv6 ospf interface**
OSPFv3 BFD Commands	**ipv6 ospf bfd-state** **ipv6 ospf bfd-state all-interfaces** **ipv6 ospf interface bfd-state** **ipv6 ospf interface bfd-state drs-only** **ipv6 ospf interface bfd-state all-neighbors**
OSPFv3 Graceful Restart Commands	**ipv6 ospf restart** **ipv6 ospf restart initiate** **ipv6 ospf restart interval** **ipv6 ospf restart-helper** **ipv6 ospf restart-helper strict-lsa-check** **show ipv6 ospf restart**

ipv6 load ospf

Loads the OSPFv3 software on the router.

ipv6 load ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> ipv6 load ospf
```

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaVrConfigTable
   alaVrConfigOspf3Status
```

ipv6 ospf admin-state

Enables or disables the OSPFv3 administrative status for the router.

ipv6 ospf admin-state {enable | disable}

Syntax Definitions

enable	Enables OSPFv3.
disable	Disables OSPFv3.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The OSPFv3 protocol should be enabled to route traffic.

Examples

```
-> ipv6 ospf admin-state enable
-> ipv6 ospf admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf	Displays OSPFv3 status and general configuration parameters.

MIB Objects

```
ospfv3GeneralGroup
   ospfv3AdminStat
```

ipv6 ospf host

Creates or deletes an OSPFv3 entry for directly attached hosts.

ipv6 ospf host *ipv6_address* **[area** *area_id***] [metric** *metric***]**

no ipv6 ospf host *ipv6_address* **area** *area_id*

Syntax Definitions

ipv6_address	The 128-bit IP address of the OSPFv3 host.
area_id	Area to which the host route belongs.
metric	The cost metric value assigned to the specified host. The valid range is 0–65535.

Defaults

parameter	default
metric	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove the record of the OSPFv3 host.
- Use this command when multiple paths exist to a host. The specified host must be directly attached to the router. A metric value is the cost of all the hops necessary for a packet to reach its destination. Routers use the metric to determine the best possible path.
- This command allows you to modify the host parameter **metric**.

Examples

```
-> ipv6 ospf host 2001::1/64 metric 10
-> no ipv6 ospf host 2001::1/64 metric 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf host	Displays information on the configured OSPFv3 hosts.

MIB Objects

```
ospfv3HostTable
   ospfv3HostStatus
   ospfv3HostAreaID
   ospfv3HostAddress
   ospfv3HostMetric
```

ipv6 ospf mtu-checking

Enables or disables Maximum Transfer Unit (MTU) checking. The MTU limits the size of a transmitted or received packet.

ipv6 ospf mtu-checking

no ipv6 ospf mtu-checking

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to disable MTU checking.
- This command is used to disable the checking for mismatch of the interface MTU while establishing a neighbor adjacency with a router. MTU mismatch occurs when a router receives packets that contain a larger MTU value than that of the interface on which adjacency is being established. The interface MTU is the largest IP datagram size (in bytes) that the interface can accept.

Examples

```
-> ipv6 ospf mtu-checking
-> no ipv6 ospf mtu-checking
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3
   alaOspf3MTUCheck
```

ipv6 ospf route-tag

Configures a tag value for the Autonomous System External (ASE) routes created.

ipv6 ospf route-tag *tag*

Syntax Definitions

tag	The set tag value. The valid range is 0–2, 147, 483, 647.

Defaults

parameter	default
tag	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows you to set a tag value for ASE routes that are learned by this OSPFv3 router. The tag value allows for quick identification.
- OSPFv3 ASE route advertisements contain a tag value field. This field allows the exchange of information between autonomous system border routers (ASBRs).

Examples

```
-> ipv6 ospf route-tag 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf	Displays OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3
   alaOspf3RedistRouteTag
```

ipv6 ospf spf-timer

Configures timers for Shortest Path First (SPF) calculation.

ipv6 ospf spf-timer [delay *delay_seconds***] [hold** *hold_seconds***]**

Syntax Definitions

delay_seconds	Specifies time (from 0 to 65535 seconds) between the reception of an OSPFv3 topology change and the start of an SPF calculation.
hold_seconds	Specifies the minimum time (from 0 to 65535 seconds) between consecutive SPF calculations.

Defaults

parameter	default
delay_seconds	5
hold_seconds	10

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows you to configure the time interval between SPF calculations.
- Use the delay timer to determine how much time to postpone an SPF calculation after the router receives a topology change.
- Use the hold timer to configure the amount of time that must elapse between consecutive SPF calculations.
- There will be no delay in the SPF calculation if either the delay timer or hold timer is set to 0. The SPF calculations will occur immediately upon the reception of a topology change and/or that back-to back SPF calculations can take place with no break in-between the two.

Examples

```
-> ipv6 ospf spf-timer delay 20 hold 35
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3
   alaOspf3TimerSpfDelay
   alaOspf3TimerSpfHold
```

ipv6 ospf virtual-link

Creates or deletes a virtual link. A virtual link restores the backbone connectivity if the backbone is not physically contiguous.

ipv6 ospf virtual-link area *area_id* **router** *router_id* **[dead-interval** *seconds***] [hello-interval** *seconds***] [retrans-interval** *seconds***] [transit-delay** *seconds***]**

no ipv6 ospf virtual-link area *area_id* **router** *router_id*

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
router_id	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
dead-interval *seconds*	Sets the virtual link dead interval. If no hello packets on this link for the set number of seconds have been received, the virtual neighbor is declared dead. The valid range is 1–2147483647.
hello-interval *seconds*	Sets the virtual link hello interval, which is the time interval between OSPFv3 hellos sent on this virtual link. The valid range is 1–65535.
retrans-interval *seconds*	Sets the virtual link retransmit interval. The router waits the set number of seconds before retransmitting OSPFv3 packets. The valid range is 0–3600.
transit-delay *seconds*	Sets the virtual link transit delay, which is the number of seconds to transmit OSPFv3 packets over this link. The valid range is 0–3600.

Defaults

parameter	default
dead-interval *seconds*	40
hello-interval *seconds*	10
retrans-interval *seconds*	5
transit-delay *seconds*	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to delete the virtual link.
- You can define areas in such a way that the backbone is no longer contiguous. In this case, the system administrator can ensure backbone connectivity physically.
- Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a

virtual link as if they were connected by an unnumbered point-to-point network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.

- If authentication is enabled, both routers at either end of the virtual link must share the same password. Simple authentication refers to the use of only clear-text passwords as an authentication method. MD5 authentication refers to the usage of message digests.
- The **dead-interval** value should be the same for all the routers on the same network. This value should be a multiple of the value provided for the **hello-interval**.

Examples

```
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 dead-interval 50
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 hello-interval 20
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 retrans-interval 20
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 transit-delay 50
-> no ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf virtual-link	Displays the virtual link information.

MIB Objects

```
ospfv3VirtIfTable
   ospfv3VirtIfAreaId
   ospfv3VirtIfNeighbor
   ospfv3VirtIfStatus
   ospfv3VirtIfRtrDeadInterval
   ospfv3VirtIfHelloInterval
   ospfv3VirtIfRetransInterval
   ospfv3VirtIfTransitDelay
```

ipv6 ospf area

Assigns an OSPFv3 interface to a specified area.

ipv6 ospf area *area_id* [**type** {**normal** | **stub** [**default-metric** *metric*] | **nssa** [**default-metric** *metric*]}] | [**summarize** [**filter**]

no ipv6 ospf area *area_id*

Syntax Definitions

area_id	A unique 32-bit value in IP address format or a unique identification number in the range 0 to 4294967295.
normal	Sets the area as a regular OSPFv3 area.
stub	Configures an OSPFv3 area as a stub area.
nssa	Configures an OSPFv3 area as a NSSA (Not-So-Stubby Area).
metric	Defines the metric to be used for default routes injected into the stub or NSSA. The range is 0 to 4294967295.
summarize	Configures the inter-area route summarization. Prefixes that fall within the summary range can be shared with another area through the summary prefix.
filter	Configure to filter the routes specified in the summarization range. These filtered routes are not advertised into another area.

Defaults

parameter	default
normal | stub | nssa	**normal**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to delete the OSPFv3 area.
- To change the area type, first delete the area, and then recreate it with the new type.
- The **default-metric** parameter defines the metric to be used for default routes injected into the stub or NSSA.

Examples

```
-> ipv6 ospf area 0.0.0.1
-> ipv6 ospf area 0.0.0.1 stub default-metric 15
-> ipv6 ospf area 0.0.0.1 type normal
-> ipv6 ospf area 0.0.0.1 type nssa
-> ipv6 ospf area 0.0.0.1 summarize 2001:1::/64
-> no ipv6 ospf area 0.0.0.1
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **nssa** keyword added.

Related Commands

show ipv6 ospf area	Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

MIB Objects

```
ospfv3AreaTable
   ospfv3ImportAsExtern
   ospfv3AreaSummary
   ospfv3StubMetric
   ospfv3AreaId
   ospfv3AreaImportAsExtern
```

ipv6 ospf area area-summary

Configures whether or not summary routes are imported into the stub or NSSA as Type-3 summary-LSAs.

ipv6 ospf area *area_id* [**area-summary** {**noareasummary** | **sendareasummary**}]

Syntax Definitions

area_id	The area ID configured for a stub or NSSA.
noareasummary	When set to this option, inter-area LSAs will neither originate or propagate into the NSSA. Only a default route will be advertised into the NSSA.
sendareasummary	When set to this option, inter-area LSAs will be summarized and propagated into the NSSA.

Defaults

parameter	default
noareasummary | sendareasummary	**sendareasummary**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ipv6 ospf area 0.0.0.1 area-summary noAreaSummary
```

Release History

Release 8.4.1; command introduced.

Related Commands

ipv6 ospf area	Assigns an OSPFv3 interface to a specified area.
show ipv6 ospf area	Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

MIB Objects

```
ospfv3AreaSummary
```

ipv6 ospf area nssa-translator-role

Configures whether or not an NSSA border router will unconditionally translate Type-7 LSAs into Type-5 LSAs.

ipv6 ospf area *area_id* [**nssa-translator-role {always | candidate}]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
always	When set to this option, NSSA border router always translates Type-7 LSAs into Type-5 LSAs regardless of the translator state of other NSSA border routers.
candidate	When set to this option, NSSA border router participates in the translator election process.

Defaults

parameter	default
always | candidate	**candidate**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

When translator role is set to **candidate**, NSSA border router invokes a translator election process. The translator is then established by the NSSA border router whose router LSA has the greatest router ID.

Examples

```
-> ipv6 ospf area 0.0.0.1 nssa-translator role always
```

Release History

Release 8.4.1; command introduced.

Related Commands

ipv6 ospf area	Assigns an OSPFv3 interface to a specified area.
show ipv6 ospf area	Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

MIB Objects

```
ospfv3AreaNssaTranslatorRole
```

ipv6 ospf area nssa-translator-stab-interval

Configures the duration for which a Type-7 translator will continue in the translator role after another NSSA border router translator has assumed the role.

ipv6 ospf area *area_id* [**nssa-translator-stab-interval** *interval*]

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
interval	NSSA translator stability interval value in seconds. The range is 0 to 4294967295.

Defaults

The default value is 40 seconds.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ipv6 ospf area 0.0.0.1 nssa-translator-stab-interval 60
```

Release History

Release 8.4.1; command introduced.

Related Commands

ipv6 ospf area	Assigns an OSPFv3 interface to a specified area.
show ipv6 ospf area	Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

MIB Objects

```
ospfv3AreaNssaTranslatorStabInterval
```

ipv6 ospf area nssa-summarize

Configures an NSSA summary of IPv6 prefix in the given area. Any NSSA LSAs within the area subsumed by IPv6 prefix will be summarized into other areas as an external LSA with a prefix of IPv6 prefix.

ipv6 ospf area *area_id* **nssa-summarize** *ipv6_address_prefix* [**filter**]

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
ipv6_address_prefix	The 128-bit IPv6 address in hexadecimal format.
filter	Use filter option to suppress the external LSA.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ipv6 ospf area 2 nssa-summarize c000::/64
```

Release History

Release 8.4.1 R03; command introduced.

Related Commands

ipv6 ospf area	Assigns an OSPFv3 interface to a specified area.
show ipv6 ospf area	Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

MIB Objects

```
ospfv3AreaAggregateTable
```

ipv6 ospf interface

Creates or deletes an OSPFv3 interface.

ipv6 ospf interface *interface_name*

no ipv6 ospf interface *interface_name*

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to delete an OSPFv3 interface.
- The interface name cannot contain spaces.

Examples

```
-> ipv6 ospf interface vlan-101
-> no ipv6 ospf interface vlan-101
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
```

ipv6 ospf interface admin-state

Enables or disables the administration status on an OSPFv3 interface.

ipv6 ospf interface *interface_name* **admin-state {enable | disable}**

no ipv6 ospf interface *interface_name*

Syntax Definitions

interface_name	The name of the interface.
enable	Enables the OSPFv3 interface.
disable	Disables the OSPFv3 interface.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to delete an OSPFv3 interface.
- The OSPFv3 interface must be enabled to participate in the OSPFv3 protocol.

Examples

```
-> ipv6 ospf interface vlan-101 admin-state enable
-> ipv6 ospf interface vlan-101 admin-state disable
-> no ipv6 ospf interface vlan-101
-> no ipv6 ospf interface vlan-101
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfAdminStat
```

ipv6 ospf interface suppress-link-lsa

Allows to suppress the announcements of the Link State Advertisements (LSAs).

ipv6 ospf interface *interface_name* **suppress-link-lsa**

no ipv6 ospf interface *interface_name* **suppress-link-lsa**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to disable LSA suppression.

Examples

```
-> ipv6 ospf interface vlan-101 suppress-link-lsa
-> no ipv6 ospf interface vlan-101 suppress-link-lsa
```

Release History

Release 8.1.1; command introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   alaOspf3SuppressLinkLsa
```

ipv6 ospf interface type

Allows to configure the type of OSPFv3 interface.

ipv6 ospf interface *interface_name* **type {broadcast | point-to-point | point-to-multipoint | nbma}**

Syntax Definitions

interface_name	The name of the interface.
broadcast	The interface is a broadcast interface.
point-to-point	The interface is a point-to-point interface.
point-to-multipoint	The interface is a point-to-multipoint interface.
nbma	The interface is a NBMA interface.

Defaults

parameter	default
broadcast | point-to-point | point-to-multipoint | nbma	**broadcast**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The OSPFv3 interface must be enabled to participate in the OSPFv3 protocol.

Examples

```
-> ipv6 ospf interface vlan-101 type nbma
-> ipv6 ospf interface vlan-101 type point-to-point
-> ipv6 ospf interface vlan-101 type point-to-multipoint
-> ipv6 ospf interface vlan-101 type broadcast
```

Release History

Release 8.1.1; command introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfStatus
   ospfv3IfType
```

ipv6 ospf neighbor

Allows to configure OSPFv3 neighbor on non-broadcast interface type. The neighbor configuration is required on NBMA and point-to-multipoint interface to run OSPFv3.

ipv6 ospf neighbor *nbr_ipv6_address* **interface** *interface_name* **{eligible | ineligible}**

no ipv6 ospf neighbor *nbr_ipv6_address*

Syntax Definitions

nbr_ipv6_address	Link-local address of the neighbor to be linked.
interface_name	The name of the interface on which the neighbor is reachable.
eligible	Indicates the neighbor is eligible to become the designated router.
ineligible	Indicates the neighbor is ineligible to become the designated router.

Defaults

parameter	default
eligible | ineligible	**eligible**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to delete the neighbor configuration.
- The OSPFv3 interface must be configured before configuring the OSPFv3 neighbor.
- This command is not applicable for broadcast interface type and is optional for point-to-point interface type.

Examples

```
-> ipv6 ospf neighbor fe80::2e0:b1ff:fe7e:5f1e interface vlan-101 eligible
-> ipv6 ospf neighbor fe80::2e0:b1ff:fe7e:5f1e interface vlan-101 ineligible
-> no ipv6 ospf neighbor fe80::2e0:b1ff:fe7e:5f1e interface vlan-101
```

Release History

Release 8.1.1; command introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.
ipv6 ospf interface admin-state	Allows to configure the type of OSPFv3 interface.

MIB Objects

```
ospfv3NbrTable
   ospfv3NbrPriority
   ospfv3NbmaNbrStatus
```

ipv6 ospf interface area

Configures an OSPFv3 area identifier for this interface.

ipv6 ospf interface *interface_name* **area** *area_id*

Syntax Definitions

interface_name	The name of the interface.
area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

An interface must be assigned to an area to become operational.

Examples

```
-> ipv6 ospf interface vlan-101 area 0.0.0.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf area	Displays either all the OSPFv3 areas, or a specified OSPFv3 area.
show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfAreaId
```

ipv6 ospf interface dead-interval

Configures the OSPFv3 interface dead interval.

ipv6 ospf interface *interface_name* **dead-interval** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The dead interval, in seconds. The valid range is 1–65535.

Defaults

parameter	default
seconds (broadcast and point-to-point)	40
seconds (NBMA and point-to-multipoint)	120

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- After the dead interval, a neighbor on this interface is considered dead if no hello packets have been received from this neighbor.
- This interval should be greater than the hello interval or multiples of the hello interval.

Examples

```
-> ipv6 ospf interface vlan-101 dead-interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf interface hello-interval	Configures the OSPFv3 interface hello interval.
show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfRtrDeadInterval
```

ipv6 ospf interface hello-interval

Configures the OSPFv3 interface hello interval.

ipv6 ospf interface *interface_name* **hello-interval** *seconds*

Syntax Definitions

interface_name	The name of the interface.
seconds	The hello interval, in seconds. The valid range is 0–65535. A value of 0 creates a passive OSPFv3 interface.

Defaults

parameter	default
seconds (broadcast and point-to-point)	10
seconds (NBMA and point-to-multipoint)	30

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This is the interval between two consecutive hello packets sent out on this interface.

Examples

```
-> ipv6 ospf interface vlan-101 hello-interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf interface dead-interval	Configures the OSPFv3 interface dead interval.
show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfHelloInterval
```

ipv6 ospf interface cost

Configures the OSPFv3 interface cost.

ipv6 ospf interface *interface_name* **cost** *cost*

Syntax Definitions

interface_name	The name of the interface.
cost	The interface cost. The valid range is 0–65535.

Defaults

parameter	default
cost	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The configured interface cost (if any) is used during OSPFv3 route calculations.

Examples

```
-> ipv6 ospf interface vlan-101 cost 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfMetricValue
```

ipv6 ospf interface priority

Configures the OSPFv3 interface priority. The priority number helps determine the eligibility of this router to become the designated router on the network.

ip ospf interface *interface_name* **priority** *priority*

Syntax Definitions

interface_name	The name of the interface.
priority	The interface priority. The valid range is 0–255.

Defaults

parameter	default
priority	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the highest priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become the designated router.

Examples

```
-> ipv6 ospf interface vlan-101 priority 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfRtrPriority
```

ipv6 ospf interface retrans-interval

Configures the OSPFv3 interface retransmit time interval.

ipv6 ospf interface *interface_name* **retrans-interval** *interval*

Syntax Definitions

interface_name	The name of the interface.
seconds	The retransmit interval, in seconds. The valid range 0–3600.

Defaults

parameter	default
interval	5

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The number of seconds between link retransmission of OSPFv3 packets on this interface.

Examples

```
-> ipv6 ospf interface vlan-101 retrans-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfRetransInterval
```

ipv6 ospf interface transit-delay

Configures the OSPFv3 interface transit time delay.

ipv6 ospf interface *interface_name* **transit-delay** *delay*

Syntax Definitions

interface_name	The name of the interface.
delay	The transit delay, in seconds. The valid range is 0–3600.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The estimated number of seconds required to transmit a link state update over this interface. This command takes into account transmission and propagation delays and must be greater than 0.

Examples

```
-> ipv6 ospf interface vlan-101 transit-delay 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfIndex
   ospfv3IfTransitDelay
```

ipv6 ospf bfd-state

Enables or disables the registration of OSPFv3 with the BFD protocol.

ipv6 ospf bfd-state {enable | disable}

Syntax Definitions

enable	Enables BFD for OSPFv3.
disable	Disables BFD for OSPFv3.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- BFD must be globally enabled for the switch and OSPFv3 must be registered with BFD at the protocol level before OSPFv3 can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and the OSPFv3 protocol acts based upon the BFD message.
- Whenever a neighbor goes down, OSPFv3 will inform BFD to remove that neighbor from the BFD active list.

Examples

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of OSPFv3 with the BFD protocol:

```
-> ipv6 ospf bfd-state enable
-> ipv6 ospf bfd-state disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ip bfd admin-state	Enables or disables the global BFD protocol status for the switch.
ipv6 ospf bfd-state all-interfaces	Enables or disables BFD for all OSPFv3 interfaces configured.
ipv6 ospf interface bfd-state	Enables or disables BFD for a specific OSPFv3 interface.
ipv6 ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
ipv6 ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
show ipv6 ospf	Displays OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3
   alaOspf3BfdStatus
```

ipv6 ospf bfd-state all-interfaces

Enables or disables BFD for all OSPFv3 interfaces in the switch configuration.

ipv6 ospf bfd-state all-interfaces {enable | disable}

Syntax Definitions

enable	Enables BFD for all the OSPFv3 interfaces.
disable	Disables BFD for all the OSPFv3 interfaces.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for OSPFv3 must be enabled before OSPFv3 can interact with BFD.

Examples

```
-> ipv6 ospf bfd-state all-interfaces enable
-> ipv6 ospf bfd-state all-interfaces disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 ospf bfd-state	Enables or disables the BFD status for the OSPFv3 protocol.
ipv6 ospf interface bfd-state	Enables or disables BFD for a specific OSPFv3 interface.
ipv6 ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
ipv6 ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
show ipv6 ospf interface	Displays configuration information for an OSPFv3 interface.

MIB Objects

```
alaProtocolOspf3
   alaOspf3BfdAllInterfaceStatus
```

ipv6 ospf interface bfd-state

Enables or disables BFD for a specific OSPFv3 interface.

ipv6 ospf interface *if_name* **bfd-state {enable | disable}**

Syntax Definitions

if_name	The name of an existing OSPFv3 interface.
enable	Enables BFD for the OSPFv3 interface.
disable	Disables BFD for the OSPFv3 interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for OSPFv3 must be enabled before OSPFv3 can interact with BFD.

Examples

```
-> ipv6 ospf interface int1 bfd-state enable
-> ipv6 ospf interface int2 bfd-state disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 ospf bfd-state	Enables or disables the BFD status for the OSPFv3 protocol.
ipv6 ospf bfd-state all-interfaces	Enables or disables BFD for all OSPFv3 interfaces configured.
ipv6 ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
ipv6 ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
show ipv6 ospf interface	Displays configuration information for an OSPFv3 interface.

MIB Objects

```
alaOspf3IfAugTable
   alaOspf3IfBfdStatus
```

ipv6 ospf interface bfd-state drs-only

Establishes BFD sessions only with neighbors that are in the full state.

ipv6 ospf interface *if_name* **bfd-state drs-only**

Syntax Definitions

if_name	The name of an existing OSPFv3 interface.

Defaults

parameter	default
drs-only	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The specified OSPFv3 interface must be enabled to interact with BFD.
- The BFD status for OSPFv3 must be enabled before OSPFv3 can interact with BFD.

Examples

```
-> ipv6 ospf interface int1 bfd-state drs-only
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 ospf bfd-state	Enables or disables the BFD status for OSPFv3 protocol.
ipv6 ospf bfd-state all-interfaces	Enables or disables BFD for all OSPFv3 interfaces configured.
ipv6 ospf interface bfd-state	Enables or disables BFD for a specific OSPFv3 interface.
ipv6 ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
show ipv6 ospf interface	Displays configuration information for an OSPFv3 interface.

MIB Objects

```
alaOspf3IfAugTable
   alaOspf3IfDrsOnly
```

ipv6 ospf interface bfd-state all-neighbors

Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

ipv6 ospf interface *if_name* **bfd-state all-neighbors {enable | disable}**

Syntax Definitions

if_name	The name of an existing OSPFv3 interface.
enable	Enables BFD sessions with all neighbors.
disable	Disables BFD sessions with all neighbors.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The specified OSPFv3 interface must be enabled to interact with BFD.
- The BFD status for OSPFv3 must be enabled before OSPFv3 can interact with BFD.

Examples

```
-> ipv6 ospf interface int1 bfd-state all-neighbors enable
-> ipv6 ospf interface int1 bfd-state all-neighbors disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 ospf bfd-state	Enables or disables the BFD status for OSPFv3 protocol.
ipv6 ospf bfd-state all-interfaces	Enables or disables BFD for all OSPFv3 interfaces configured.
ipv6 ospf interface bfd-state	Enables or disables BFD for a specific OSPFv3 interface.
ipv6 ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
show ipv6 ospf interface	Displays configuration information for an OSPFv3 interface.

MIB Objects

```
alaOspf3IfAugTable
   alaOspf3IfDrsOnly
```

show ipv6 ospf

Displays the OSPFv3 status and general configuration parameters.

show ipv6 ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command is used to display the general configuration parameters of the OSPFv3 router. See the Related Commands section below for commands that are used to modify the displayed parameters.

Examples

```
-> show ipv6 ospf
Status                          = Enabled,
Router ID                       = 30.1.1.2,
# Areas                         = 1,
# Interfaces                    = 3,
Area Border Router              = No,
AS Border Router                = No,
External Route Tag              = 0,
SPF Hold (seconds)              = 10,
SPF Delay (seconds)             = 5,
MTU checking                    = Enabled,
BFD Status                      = Disabled,
# SPF calculations performed    = 34,
Last SPF run (seconds ago)      = N/A,
# of routes                     = 1,
# of AS external LSAs           = 0,
# of neighbors that are in:
  Full state                    = 1,
  Loading state                 = 0,
  Exchange state                = 0,
  Exstart state                 = 0,
  2way state                    = 0,
  Init state                    = 0,
  Attempt state                 = 0,
  Down state                    = 0,
Restart Support                 = Enabled,
Restart Status                  = Restating,
Restart Helper Support          = Enabled,
Restart Helper Status           = NotHelping
```

output definitions

Status	Displays whether OSPFv3 is currently enabled or disabled on the router.
Router Id	The unique identification for the router.
# Areas	Number of areas to which the router belongs.
# Interface	Number of interfaces participating in OSPFv3.
Area Border Router	Displays whether the router status is an area router or not.
AS Border Router	Displays whether the area Autonomous System Border Router status of this router is enabled or disabled.
External Route Tag	Displays the route tag for this router.
SPF Hold (seconds)	Displays the time in seconds between the reception of an OSPFv3 topology change and the start of a SPF calculation.
SPF Delay (seconds)	Displays the time in seconds between consecutive SPF calculations.
MTU Checking	Displays whether Maximum Transfer Unit checking is enabled or disabled.
BFD Status	Displays whether BFD monitoring is enabled or disabled for OSPF.
# SPF calculations performed	Displays the number of SPF calculation performed.
Last SPF run (seconds ago)	N/A
# of routes	The total number of OSPFv3 routes known to this router.
# of AS external LSAs	The number of external routes learned from outside the router's Autonomous System (AS).
# of neighbors that are in:	
Full state	Displays the number of neighbor routers that are in Full state.
Loading state	Displays the number of neighbor routers that are in Loading state.
Exchange state	Displays the number of neighbor routers that are in Exchange state.
Exstart state	Displays the number of neighbor routers that are in Exstart state.
2way state	Displays the number of neighbor routers that are in 2way state.
Init state	Displays the number of neighbor routers that are in Init state.
Attempt state	Displays the number of neighbor routers that are in Attempt state.
Down state	Displays the number of neighbor routers that are in Down state.
Restart Support	Indicates if graceful restart feature is enabled or disabled on an OSPFv3 router.
Restart Status	Displays the OSPFv3 graceful restart status.
Restart Helper Support	Indicates whether the router is acting as a restart helper for the neighbor.
Restart Helper Status	Displays the OSPFv3 graceful restart helper status.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1: OSPFv3 graceful restart fields added.

Related Commands

ipv6 ospf admin-state	Enables or disables the administration of OSPFv3 on the router.
ip router router-id	Configures the router ID for the router.
ipv6 ospf route-tag	Configures a tag value for Autonomous System External (ASE) routes created.
ipv6 ospf spf-timer	Configures timers for SPF calculation.
ipv6 ospf mtu-checking	Enables or disables the use of Maximum Transfer Unit (MTU) checking.
ipv6 ospf bfd-state	Enables or disables the registration of OSPFv3 with the BFD protocol.
ipv6 ospf restart	Configures graceful restart feature on an OSPFv3 router.
ipv6 ospf restart-helper	Enables the graceful restart helper functionality.

MIB Objects

```
ospfv3GeneralGroup
   ospfv3RouterId
   ospfv3AdminStat
   ospfv3VersionNumber
   ospfv3AreaBdrRtrStatus
   ospfv3ASBdrRtrStatus
   ospfv3OriginateNewLsas
   ospfv3RxNewLsas
   ospfv3ExitOverflowInterval
alaProtocolOspf3
   alaOspf3RedistAdminStatus
   alaOspf3RedistRouteTag
   alaOspf3TimerSpfDelay
   alaOspf3TimerSpfHold
   alaOspf3MTUCheck
   alaOspf3BfdStatus
   ospfv3RestartSupport
   ospfv3RestartStatus
   alaOspf3RestartHelperSupport
   alaOspf3RestartHelperStatus
```

show ipv6 ospf border-routers

Displays information regarding all or specified border routers.

show ipv6 ospf border-routers [area *area_id***] [router** *router_id***]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
router_id	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display a list of border routers known by this OSPFv3 router.
- By using the optional parameters, you can display the border routers using the specified parameter. For example, to find a router using a router ID of 1.1.1.1, enter the command using the router ID of 1.1.1.1 as a search criteria.
- See the Related Commands sections below to modify the list.

Examples

```
-> show ipv6 ospf border-routers

Router ID          Area           Metric   Type
---------------+---------------+--------+---------
6.6.6.6            0.0.0.0          2      INTRA
6.6.6.6            0.0.0.1          2      INTRA
        fe80::2d0:95ff:fee2:6bda -> pseudo1
        fe80::2d0:95ff:fee2:6bda -> pseudo2
```

output definitions

Router ID	The unique identification for the router.
Area	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
Metric	The metric used by the routes.
Type	The type of routes specified (intra or inter).

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

N/A

show ipv6 ospf host

Displays information on the configured OSPFv3 hosts.

show ipv6 ospf host [*ipv6_address***]**

Syntax Definitions

ipv6_address	A 128-bit IP address for a directly attached host.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display general information for OSPFv3 hosts directly attached to this router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ipv6 ospf host

Area             Metric   Address
---------------+-------+-----------
0.0.0.1            1      2001::1/64
```

output definitions

Area	A 32-bit IP address for a directly attached host. This can be set using the **ipv6 ospf host** command.
Metric	The metric assigned to the host. Metric is set using the **ipv6 ospf host** command.
Address	IPV6 address of the host.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf host	Creates or deletes an OSPFv3 entry for directly attached hosts.

MIB Objects

```
ospfv3HostTable
   ospfv3HostIpAddress
   ospfv3HostMetric
   ospfHostStatus
   ospfv3HostAreaID
```

show ipv6 ospf lsdb

Displays Link State Advertisements (LSAs) in the Link State Database (LSDB) associated with each area.

show ipv6 ospf lsdb [area *area_id***] [rtr | net | netsum | asbrsum] [linkstate-id** *ls_id***] [router-id** *router_id***]**

Syntax Definitions

area_id	A unique 32-bit value in IP address format.
rtr	Specifies router LSAs.
net	Specifies network LSAs.
netsum	Specifies network summary LSAs.
asbrsum	Specifies Autonomous System Border Router summary LSAs.
ls_id	The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.
router_id	The Router ID. The ID is a unique 32-bit value such as an IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display the LSDB of the OSPFv3 router. It can be used for OSPFv3 debugging, specifically to narrow down sections of an area to determine which sections are receiving the specified LSAs. You can specify the parameters of only the area LSDB using the optional command parameters.
- You can view LSAs by specifying either a link state identifier or a router identifier. However, when specifying a router ID, you also need to supply a valid link state ID.

Examples

```
-> show ipv6 ospf lsdb

Area             Type       Link ID      Advertising Rtr  Sequence #   Age

----------------+----------+------------+-----------------+----------+----------
0.0.0.0          Router     0            1.1.1.1           8000020f     1117
0.0.0.0          Router     0            3.3.3.3           80000208     1121
0.0.0.0          Router     0            5.5.5.5           800001f1     1117
```

```
0.0.0.0          Router     0            30.30.30.30       800000da     1115
```

output definitions

Area	The identification of the area to which the router belongs.
Type	The protocol type from where the route was learned.
Link Id	The Link state ID. The ID is a unique 32-bit value expressed as an IPv6 address. This number is used as a record in the link state database.
Advertising Rtr	The ID of the router that advertises the routes.
Sequence #	The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).
Age	The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf admin-state	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
ospfv3AsLsdbTable
   ospfv3AsLsdbAreaId
   ospfv3AsLsdbType
   ospfv3AsLsdbLsid
   ospfv3AsLsdbRouterId
   ospfv3AsLsdbAdvertisement
   ospfv3AsLsdbSequence
   ospfv3AsLsdbAge
```

show ipv6 ospf neighbor

Displays information on OSPFv3 non-virtual neighbors.

show ipv6 ospf neighbor [router *ipv4_address***][interface** *interface_name***]**

Syntax Definitions

ipv4_address	A 32-bit router ID of the neighboring router.
interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to display all non-virtual neighbors of the OSPFv3 router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ipv6 ospf neighbor
Router ID        Area/Transit Area   State  Interface
----------------+-------------------+-----+---------------------------------
1.1.1.1          0.0.0.0              FULL  vlan-2071
3.3.3.3          0.0.0.0              FULL  vlan-2071
5.5.5.5          0.0.0.0              FULL  vlan-2071
23.23.23.23      0.0.0.1              FULL  vlan-2055
23.23.23.23      0.0.0.1              FULL  vlan-2056
24.24.24.24      0.0.0.1              FULL  vlan-2065
24.24.24.24      0.0.0.1              FULL  vlan-2066
```

output definitions

Router ID	The unique identification for the router.
Area/Transit Area	The area identifier.
State	The state of the OSPFv3 neighbor adjacency.
Interface	The name of the interface.

```
-> show ipv6 ospf neighbor router 24.24.24.24
Router ID        Area/Transit Area   State  Interface
----------------+-------------------+-----+--------------
24.24.24.24      0.0.0.1              FULL  vlan-2070
24.24.24.24      0.0.0.1              FULL  vlan-2073
```

output definitions

Router ID	The unique identification for the router.
Area/Transit Area	The area identifier.
State	The state of the OSPFv3 neighbor adjacency.
Interface	The name of the interface.

```
-> show ipv6 ospf neighbor router 1.1.1.1 interface v14
Details for Neighbor 1.1.1.1
State                            = FULL,
Type                             = Dynamic,
Interface                        = v14,
Neighbor i/f index               = 21,
Priority                         = 1,
Address                          = fe80::eae7:32ff:fe11:cc69,
Neighbor is reporting DR as      = 30.1.1.2,
Neighbor is reporting BDR as     = 1.1.1.1,
Neighbor is Master/Slave         = Master,
Seconds since last Hello seen    = 8,
# of LSAs on retransmit list     = 0,
# of LSAs on request list        = 0,
# of State Changes               = 6,
Restart Helper Status            = NotHelping,
Restart Age                      = 0 sec,
Last Restart Helper Exit Reason  = None
Neighbor options:
                                 V6 bit is set
                                 E bit is set
                                 MC bit is not set
                                 N bit is not set
                                 R bit is set
                                 DC bit is not set
```

output definitions

State	The state of the OSPFv3 neighbor adjacency.
Type	Specifies the type of neighbor.
Interface	The name of the interface.
Neighbor i/f index	The unique value assigned to the neighbor.
Priority	The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.
Address	The IPv6 address of the host.
Neighbor is reporting DR as	The address of the neighbors designated router.
Neighbor is reporting BDR as	The address of the neighbors Backup Designated Router.
Neighbor is Master/Slave	The role the neighbor has with the local router during DD Exchange, which can be Master or Slave.
Seconds since last Hello seen	The amount of time (in seconds) since the last HELLO messages was received from this neighbor.
# of LSAs on retransmit list	The number of Link State updates to the neighbor that need to be retransmitted by the OSPFv3 router.
# of LSAs on request list	The number of Link State requests to this neighbor that have not received a response from this neighbor.

output definitions (continued)

# of State Changes	The number of times this OSPFv3 interface has changed its state.
Restart Helper Status	Indicates whether the router is acting as a restart helper for the neighbor.
Restart Age	The remaining time, in seconds, for the current OSPFv3 restart interval if the router is acting as a restart helper for the neighbor.
Last Restart Helper Exit Reason	The outcome of the last attempt at acting as a restart helper for the neighbor.
Neighbor options	If set: V6 - V6 support R - If clear, a node can participate in OSPFv3 topology distribution without being used to forward transit traffic N - Type 7 LSA support MC - Multicast support E - External routes support DC - Demand circuit support

Release History

Release 7.1.1; command was introduced.
Release 8.4.1: OSPFv3 graceful restart fields added.

Related Commands

show ipv6 ospf	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
ospfv3NbrTable
   ospfNbrAddress
   ospfv3NbrRtrId
   ospfv3NbrOptions
   ospfv3NbrPriority
   ospfv3NbrState
   ospfv3NbrEvents
   ospfv3NbrHelloSuppressed
   ospfv3NbrRestartHelperStatus
   ospfv3NbrRestartHelperAge
   ospfv3NbrRestartHelperExitReason
   ospfv3VirtNbrRestartHelperStatus
   ospfv3VirtNbrRestartHelperAge
   ospfv3VirtNbrRestartHelperExitReason
```

show ipv6 ospf routes

Displays the OSPFv3 routes known to the router.

show ipv6 ospf routes [prefix *ipv6_address_prefix***][gateway** *gateway***]**

Syntax Definitions

ipv6_address_prefix	The 128-bit IPv6 address of the route destination in hexadecimal format.
gateway	The next hop IPv6 address for this router.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- If no variables are entered, all routes are displayed.
- If the variables are entered, then only routes matching the specified criteria are shown.
- All the variables described above must be entered for a route match. If all of the variables are not entered, an error message is returned.

Examples

```
-> show ipv6 ospf routes
                                                          Metric
Prefix                                    Path Type       1 : 2
------------------------------------------+----------+-------------------
::/ 0                                       INTER        2 : -
         fe80::2d0:95ff:fee0:710c -> vlan-2071
2051::/64                                   INTRA        2 : -
         fe80::2d0:95ff:feac:a59f -> vlan-2055
         fe80::2d0:95ff:feac:a59f -> vlan-2056
         fe80::2d0:95ff:fed7:747e -> vlan-2065
         fe80::2d0:95ff:fed7:747e -> vlan-2066
```

output definitions

Prefix	The destination address of the IPv6 route in the hexadecimal format.
Path Type	The type of routes specified (intra or inter).
Metric	The cost of the route.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf admin-state	Displays the OSPFv3 status and general configuration parameters.

MIB Objects

N/A

show ipv6 ospf virtual-link

Displays virtual link information. A virtual link is used to connect OSPFv3 backbone routers that are not physically contiguous.

show ipv6 ospf virtual-link [*router_id***]**

Syntax Definitions

router_id	The router ID of the remote end of the virtual link.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 ospf virtual-link
                                      Intf   Nbr
Transit Area     Peer Router ID    State  State   Cost
----------------+----------------+------+-------+------+
0.0.0.1          6.6.6.6           P2P     FULL    2
```

output definitions

Transit Area	The area identification for the area assigned to the virtual link.
Peer Router ID	The destination router identification for the virtual link.
Intf State	The state of the virtual link with regards to the local router.
Nbr State	The state of the virtual link adjacency.
Cost	The cost metric of the route.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf virtual-link	Creates or deletes a virtual link.

MIB Objects

```
ospfv3VirtIfTable
   ospfv3VirtIfAreaId
   ospfv3VirtIfNeighbor
   ospfv3VirtIfState
```

show ipv6 ospf area

Displays either all OSPFv3 areas, or a specified OSPFv3 area.

show ipv6 ospf area [*area_id*]

Syntax Definitions

area_id	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Allows you to view the details of a specified OSPFv3 area.
- If an OSPFv3 area is not specified, all known areas for the OSPFv3 router will be displayed.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ipv6 ospf area
                          Stub     Number of
 Area ID          Type    Metric    Interfaces
----------------+-------+--------+---------------
 0.0.0.0          Normal  NA           2
 0.0.0.1          Stub    1000000      2
 0.0.0.2          Nssa    1000         1

-> show ipv6 ospf area 0.0.0.0
Details for Area 0.0.0.0

Area Type                               = Normal,
Area Stub Metric                        = 0,
# of SPF calculations                   = 0,
# Interfaces                            = 2,
# Router LSAs                           = 0,
# Network LSAs                          = 0,
# Intra-area-prefix LSAs                = 0,
# Inter-area-prefix LSAs                = 0,
# Inter-area-router LSAs                = 0,
# hosts                                 = 0,
# ABRs                                  = 0,
# ASBRs                                 = 0,
Summarization ranges                    = 0
```

```
-> show ipv6 ospf area 0.0.0.1
Details for Area 0.0.0.1

Area Type                                = Stub,
Area Stub Metric                         = 1000000,
# of SPF calculations                    = 2,
# Interfaces                             = 2,
# Router LSAs                            = 0,
# Network LSAs                           = 0,
# Intra-area-prefix LSAs                 = 0,
# Inter-area-prefix LSAs                 = 0,
# Inter-area-router LSAs                 = 0,
# hosts                                  = 0,
# ABRs                                   = 0,
# ASBRs                                  = 0,
Summarization ranges                     = 2
        Range #0, address 2001::/64, filter no
        Range #1, address 2002::/64, filter yes
Import Area Summaries                    = Enabled


-> show ipv6 ospf area 0.0.0.2
Details for Area 0.0.0.2

Area Type                                = NSSA,
Area Stub Metric                         = 1000,
# of SPF calculations                    = 2,
# Interfaces                             = 1,
# Router LSAs                            = 3,
# Network LSAs                           = 2,
# Intra-area-prefix LSAs                 = 2,
# Inter-area-prefix LSAs                 = 1,
# Inter-area-router LSAs                 = 0,
# hosts                                  = 0,
# ABRs                                   = 1,
# ASBRs                                  = 2,
Summarization ranges                     = 0
Import Area Summaries                    = Enabled
NSSA Translator Role                     = Candidate
NSSA Translator State                    = Elected
# NSSA Translator State Changes          = 1,
```

output definitions

Area Type	The area type. This field will be **normal**, **stub**, or **NSSA**.
Area Stub Metric	Indicates whether the area is enabled or disabled.
# Router LSAs	The total number of Link State Advertisements for the Area.
# Network LSAs	The total number of inter-area Link State Advertisements.
# of SPF calculations	The number of times the area has calculated the Shortest Path.
# Interfaces	The number of OSPFv3 interfaces.
# Intra-area-prefix LSAs	The number of intra-area-prefix LSAs, which associates a list of IPv6 address prefixes with a router by referencing a router-LSA.
# Inter-area-prefix LSAs	The number of inter-area-prefix LSAs.Corresponds to Type 3 summary-LSA of OSPFv3.

output definitions (continued)

# Inter-area-router LSAs	The number of inter-area-router LSAs. Corresponds to Type 4 summary-LSA of OSPFv3.
# hosts	The number of directly attached hosts.
# ABRs	Number of Area Border Routers in the area.
# ASBRs	Number of Autonomous System Border Routers in the area.
Summarization ranges	The range of prefixes summarized in to the area.
Import Area Summaries	Specifies whether or not summary routes are imported into the stub or NSSA as Type-3 summary-LSAs.
NSSA Translator Role	Specifies the NSSA translator role: **Candidate** or **Always**
NSSA Translator State	Indicates if and how an NSSA border router is performing NSSA translation (**ipv6 ospf area nssa-translator-role**) of NSSA-LSAs into AS-External-LSAs: Enabled, Elected, Disabled. **Enabled** indicates that the NSSA border router's translator role has been set to 'always'. **Elected** indicates that a candidate NSSA border router is translating NSSA-LSAs into AS-External-LSAs. **Disabled** indicates that a candidate NSSA Border router is not translating NSSA-LSAs into AS-External-LSAs.
# NSSA Translator State Changes	Indicates the number of translator state changes that have occurred since the last start-up of the OSPFv3 routing process.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; NSSA related fields added.

Related Commands

ipv6 ospf area	Creates or deletes an OSPFv3 area, assigning default metric, cost, and type.
show ipv6 ospf interface	Displays OSPFv3 interface information.

MIB Objects

```
ospfv3AreaTable
   ospfv3AreaId
   ospfv3ImportAsExtern
   ospfv3SpfRuns
   ospfv3AreaBdrRtrCount
   ospfv3AreaSummary
   ospfv3AreaStatus
   ospfv3AreaNssaTranslatorRole
   ospfv3AreaNssaTranslatorState
   ospfv3AreaNssaTranslatorStabInterval
   ospfv3AreaNssaTranslatorEvents
```

show ipv6 ospf interface

Displays OSPFv3 interface information.

show ipv6 ospf interface [*interface_name***]**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Not specifying the interface name displays all known interfaces for the OSPFv3 router.

Examples

```
-> show ipv6 ospf interface
                                                  IPv6
                                        Admin     Intf     Intf    Intf       BFD
 Name      DR Router ID  BDR Router ID  Status    Status   Type    State     Status
----------+-------------+--------------+---------+------+------+---------+----------
vlan-2071    5.5.5.5       0.0.0.0      Enabled    Up     BCAST   DR       Enabled
vlan-2055    7.7.7.7       5.5.5.5      Enabled    Up     BCAST   BDR      Enabled
vlan-2056    7.7.7.7       5.5.5.5      Enabled    Up     BCAST   BDR      Disabled
```

output definitions

Name	The name of the interface.
DR Router ID	The designated router address on this network segment. Make sure you configure a VLAN for the router IP. (See Chapter 5, "VLAN Management Commands," for more information.)
BDR Router ID	The IP address of the backup designated router.
Admin Status	The current administration status of the interface, either **enabled** or **disabled**.
IPv6 Intf Status	Indicates whether the interface is an active OSPFv3 interface.
Intf Type	Whether the interface is assigned to a VLAN or tunnel.
Intf State	The current state of the OSPFv3 interface. It will be **DR, BDR, other.**
BFD Status	The current status of BFD for the OSPFv3 interface.

```
-> show ipv6 ospf interface vlan-2071
Details for Intf 'vlan-2071'

Name                            = vlan-2071,
Type                            = BROADCAST,
Admin Status                    = Enabled,
IPv6 Interface Status           = Up,
Oper Status                     = Up,
State                           = DR,
Area                            = 0.0.0.0,
Priority                        = 100,
Cost                            = 1,
Designated Router               = 3.3.3.3,
Backup Designated Router        = 0.0.0.0,
Hello Interval                  = 1,
Router Dead Interval            = 4,
Retransmit Interval             = 5,
Transit Delay                   = 1,
Ifindex                         = 17
IPv6 'ifindex'                  = 2071,
MTU                             = 1500,
Link LSA suppression            = disabled,
BFD Status                      = disabled,
# of attached neighbors         = 0,
# of state changes              = 0,
Link-local address              = fe80::2efa:a2ff:fe13:e402
```

Output fields when an IP address or interface name is specified are described below:

output definitions

Type	The OSPFv3 interface type, which can be Broadcast, NBMA, Point-to-Point, or Point-to-Multipoint.
Admin Status	The current administrative status of the interface, either **enabled** or **disabled**.
IPv6 Interface Status	The current administrative status of the IPv6 interface, either **up** or **down**.
Oper Status	Indicates whether the interface is an active OSPFv3 interface.
State	The current state of the OSPFv3 interface. It will be **down**, **up**, **dp**, **dr**, or **other**.
Area	The area identification number to which the interface is assigned. This field is not applicable if an interface has not yet been assigned to an area.
Priority	The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.
Cost	The cost added to routes learned on this interface.
Designated Router	The identification number of the designated router.
Backup Designated Router	The identification number of the backup designated router.
Hello Interval	The number of seconds between hello messages sent out on the interface.
Router Dead Interval	The number of seconds the interface waits for hello messages received from a neighbor before declaring the neighbor as dead.

output definitions (continued)

Retransmit Interval	The number of seconds the interface waits before resending hello messages.
Transit Delay	The estimated number of seconds required to transmit a link state update over this interface.
Ifindex	The unique value assigned to an interface.
IPv6 'ifindex'	The unique value assigned to an IPv6 interface.
MTU	The Maximum Transfer Unit (in bytes) for the interface.
Link LSA suppression	Whether or not (enabled or disabled) link LSA origination is suppressed for broadcast or NBMA interface types.
BFD Status	The status of BFD on this interface.
# of attached neighbors	The number of OSPFv3 neighbors in the initialization state.
# of state changes	The number of times this OSPFv3 interface has changed its state.
Link-local address	A globally unique IPv6 address.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; **bfd status** field added.

Related Commands

ipv6 ospf interface	Creates and deletes an OSPFv3 interface.
ipv6 ospf interface dead-interval	Configures the OSPFv3 interface dead interval.
ipv6 ospf interface hello-interval	Configures the OSPFv3 interface hello interval.
ipv6 ospf interface cost	Configures the OSPFv3 interface cost.
ipv6 ospf interface priority	Configures the OSPFv3 interface priority.
ipv6 ospf interface retrans-interval	Configures the OSPFv3 interface retransmit interval.
ipv6 ospf interface transit-delay	Configures the OSPFv3 interface transit delay.
ipv6 ospf interface area	Configures an OSPFv3 interface area.
ipv6 ospf interface admin-state	Enables or disables the administration status on an OSPFv3 interface.
ipv6 ospf interface suppress-link-lsa	Configures whether or not link LSA origination is suppressed for broadcast or NBMA interface types.
ipv6 ospf interface bfd-state	Enables or disables the status of BFD for an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
   ospfv3IfAreaId
   ospfv3IfType
   ospfv3IfAdminStat
   ospfv3IfRtrPriority
   ospfv3IfTransitDelay
   ospfv3IfRetransInterval
   ospfv3IfHelloInterval
   ospfv3IfRtrDeadInterval
   ospfv3IfPollInterval
   ospfv3IfState
   ospfv3IfDesignatedRouter
   ospfv3IfBackupDesignatedRouter
   ospfv3IfEvents
   ospfv3IfStatus
   ospfv3IfLinkLSASuppression
alaOspf3IfAugTable
   alaOspf3IfBfdStatus
```

ipv6 ospf restart

Configures graceful restart feature on an OSPFv3 router.

ipv6 ospf restart

Syntax Definitions

N/A

Defaults

Graceful restart is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to disable support for the graceful restart feature on an OSPFv3 router.
- The minimum hardware configuration for this command is a dual CMM configuration. The chassis based products (OmniSwitch 9900) running in a standalone or VC-1 mode must have dual CMMs. Stackable switches (OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 6900) or chassis based switches running with single CMM must have two or more chassis in the VC.
- This command enables both planned and unplanned restarts.

Examples

```
-> ipv6 ospf restart
-> no ipv6 ospf restart
```

Release History

Release 8.4.1; command introduced

Related Commands

show ipv6 ospf restart	Displays the OSPFv3 graceful restart related configuration and status.
show ipv6 ospf	Displays the OSPFv3 status and general configuration parameters.
show ipv6 ospf neighbor	Displays information on OSPFv3 non-virtual neighbors.

MIB Objects

```
ospfv3RestartSupport
ospfv3RestartStatus
ospfv3RestartAge
ospfv3RestartExitReason
ospfv3RestartTime
```

ipv6 ospf restart initiate

Initiates a planned OSPFv3 graceful restart.

ipv6 ospf restart initiate

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command must be executed before executing the **takeover** or **vctakeover** command.

Example

```
-> ipv6 ospf restart initiate
```

Release History

Release 8.4.1; command introduced

Related Commands

show ipv6 ospf restart	Displays the OSPFv3 graceful restart related configuration and status.

MIB Objects

```
alaOspf3RestartInitiate
```

ipv6 ospf restart interval

Configures the grace period for achieving a graceful OSPFv3 restart.

ipv6 ospf restart interval [*seconds***]**

Syntax Definitions

seconds	Restart timeout interval. The valid range is 1–1800 seconds.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Restart interval must be configured based on the databases size, number of neighbors, and number of OSPFv3 areas of the restarting router. If this is configured too low, there is a chance that graceful restart may fail prematurely.

Example

```
-> ipv6 ospf restart interval 180
-> no ipv6 ospf restart interval
```

Release History

Release 8.4.1; command introduced

Related Commands

ipv6 ospf restart	Configures graceful restart feature on an OSPFv3 router.
show ipv6 ospf restart	Displays the OSPFv3 graceful restart related configuration and status.

MIB Objects

```
ospfv3RestartInterval
```

ipv6 ospf restart-helper

Enables the graceful restart helper functionality.

ipv6 ospf restart-helper

Syntax Definitions

N/A

Defaults

By default, graceful restart helper functionality is enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to disable restart helper functionality.
- A router that has configured as a helper may reject helping or stop helping in the half way if there is any topology change in the OSPFv3 network.
- The graceful restart helper does not have a requirement of having dual CMMs.

Examples

```
-> ipv6 ospf restart-helper
-> no ipv6 ospf restart-helper
```

Release History

Release 8.4.1; command introduced

Related Commands

ipv6 ospf restart	Configures graceful restart feature on an OSPFv3 router.
ipv6 ospf restart-helper strict-lsa-check	Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.
show ipv6 ospf restart	Displays the OSPFv3 graceful restart related configuration and status.

MIB Objects

```
alaOspf3RestartHelperSupport
alaOspf3RestartHelperStatus
ospfv3NbrRestartHelperStatus
ospfv3NbrRestartHelperAge
ospfv3NbrRestartHelperExitReason
ospfv3VirtNbrRestartHelperStatus
ospfv3VirtNbrRestartHelperAge
ospfv3VirtNbrRestartHelperExitReason
```

ipv6 ospf restart-helper strict-lsa-check

Enables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

ipv6 ospf restart-helper strict-lsa-check

Syntax Definitions

N/A

Defaults

By default, strict-lsa-checking is enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the no form of the command to disable this functionality.
- Disabling this functionality may create sub-optimal or black hole routes during the graceful restart period.
- This functionality does not have a requirement of having dual CMMs.

Examples

```
-> ipv6 ospf restart-helper strict-lsa-check
-> no ipv6 ospf restart-helper strict-lsa-check
```

Release History

Release 8.4.1; command introduced

Related Commands

ipv6 ospf restart	Configures graceful restart feature on an OSPFv3 router.
ipv6 ospf restart-helper	Administratively enables the capability of an OSPFv3 router to operate in helper mode in response to a router performing a graceful restart.
show ipv6 ospf restart	Displays the OSPFv3 graceful restart related configuration and status.

MIB Objects

```
ospfv3RestartStrictLsaChecking
```

show ipv6 ospf restart

Displays the OSPFv3 graceful restart related configuration and status.

show ipv6 ospf restart

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 ospf restart
Restart Support                 = Enabled (planned-unplanned),
Restart Status                  = Not Restarting,
Restart Interval                = 120,
Restart Age                     = 0,
Last Restart Exit Reason        = None,
Restart Helper Support          = Enabled,
Restart Helper Strict Checking  = Enabled,
Restart Helper Status           = NotHelping,
Time Since Exit Reason Updated  = 21:09:58
```

output definitions

Restart Support	The administrative status of OSPFv3 graceful restart.
Restart Status	The current status of OSPFv3 graceful restart, which can be **Not Restarting**, **Unplanned Restart** (after a CMM takeover), or **Planned Restart** (before CMM takeover).
Restart Interval	The configured OSPFv3 restart timeout interval, in seconds.
Restart Age	The remaining time, in seconds, for the current OSPFv3 graceful restart interval.
Last Restart Exit Reason	The outcome of the last attempt at a graceful restart. If the value is **None**, then no restart has yet been attempted. If the value is **In Progress**, then a restart attempt is currently underway. Other possible values include **Completed** (successfully completed), **Timed Out** (timed out), and **Topology Changed** (aborted due to topology change).
Restart Helper Support	The administrative status of the capability of an OSPFv3 router to operate in helper mode in response to a router performing a graceful restart.

output definitions (continued)

Restart Helper Strict Checking	The administrative status of whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.
Restart Helper Status	Indicates whether the router is acting as a graceful restart helper for the neighbor.
Time Since Exit Reason Updated	The value of system up time on the most recent occasion at which the last restart exit reason was updated.

Release History

Release 8.4.1; command introduced

Related Commands

ipv6 ospf restart	Configures graceful restart feature on an OSPFv3 router.

MIB Objects

```
alaOspf3RestartHelperSupport
ospfv3RestartInterval
ospfv3RestartStatus
ospfv3RestartAge
ospfv3RestartExitReason
alaOspf3RestartHelperSupport
ospfv3RestartStrictLsaChecking
alaOspf3RestartHelperStatus
ospfv3RestartTime
```

28 IS-IS Commands

Intermediate System-Intermediate System (IS-IS) is a shortest path first (SPF) or link-state protocol. IS-IS is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS) for IP (IPv4 and IPv6) as well as OSI environments. This feature allows a single routing protocol to support pure IP and OSI environments, and dual environments. Integrated IS-IS is also deployed extensively in an IP-only environment.

Each participating router distributes its local state (that is, the usable interfaces of the router and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. IS-IS routers have adjacencies with other routers on point-to-point links. In a multi-access network, routers report their adjacencies to a Designated Intermediate System (DIS), which generates an additional Link State PDU (LSP), commonly known as the pseudo-node LSP. The DIS is responsible for flooding the LAN with LSP and also for synchronizing the entire AS topology. This database is built from the collected link state advertisements of all routers.

IS-IS is a hierarchical protocol where the autonomous system is divided into multiple areas to reduce the size of the Routing table. Routing within an area is referred to as Level-1 routing and that between two or more areas is referred to as Level 2 routing. Each area runs a separate copy of the basic link-state routing algorithm.

The OmniSwitch version of IS-IS complies with RFC 1142.

MIB information for the IP commands is as follows:

Filename: ALCATEL-IND1-VIRTUALROUTER-MIB.mib
Module: alcatelIND1VirtualRouterMIB

Filename: ALCATEL-IND1-ISIS-MIB.mib
Module: timetraIsisMIBModule

Filename: ISIS-MIB.mib
Module: isisMIB

A summary of the available commands is listed here:

Global IS-IS Commands	**ip load isis** **ip isis admin-state** **ip isis area-id** **ip isis level-capability** **ip isis auth-check** **ip isis auth-type** **ip isis csnp-auth** **ip isis hello-auth** **ip isis psnp-auth** **ip isis lsp-lifetime** **ip isis lsp-wait** **ip isis spf-wait** **ip isis summary-address** **ip isis overload** **ip isis overload-on-boot** **ip isis graceful-restart** **ip isis graceful-restart helper** **ip isis strict-adjacency-check** **ip isis level auth-type** **ip isis level hello-auth** **ip isis level csnp-auth** **ip isis level psnp-auth** **ip isis level wide-metrics-only**
IPv4 and IPv6 Commands	**ip isis activate-ipv6|ipv4** **ip isis vlan** **ip isis vlan admin-state** **ip isis vlan interface-type** **ip isis vlan csnp-interval** **ip isis vlan hello-auth-type** **ip isis vlan level-capability** **ip isis vlan lsp-pacing-interval** **ip isis vlan passive** **ip isis vlan retransmit-interval** **ip isis vlan default-type** **ip isis vlan level hello-auth-type** **ip isis vlan level hello-interval** **ip isis vlan level hello-multiplier** **ip isis vlan level metric** **ip isis vlan level passive** **ip isis vlan level priority** **ip isis summary-address6**
IS-IS BFD Commands	**ip isis bfd-state** **ip isis bfd-state all-vlans** **ip isis vlan bfd-state**

Show Commands	**show ip isis adjacency** **show ip isis database** **show ip isis hostname** **show ip isis routes** **show ip isis routes6** **show ip isis spf** **show ip isis spf-log** **show ip isis statistics** **show ip isis status** **show ip isis summary-address** **show ip isis vlan** **show ip isis summary-address6**
Clear Commands	**clear ip isis adjacency** **clear ip isis lsp-database** **clear ip isis spf-log** **clear ip isis statistics**
M-ISIS (Multi Topology) Commands	**ip isis multi-topology**

ip load isis

Loads the IS-IS software on the router.

ip load isis

Syntax Definitions

N/A

Defaults

By default, IS-IS is not loaded on the switch.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- You need to load IS-IS on the switch before executing any IS-IS configuration command.
- To unload IS-IS, remove all the IS-IS configuration from “boot.cfg”.

Examples

```
-> ip load isis
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip protocols	Displays switch routing protocol information and status.

MIB Objects

```
alaVrConfigTable
   alaVrConfigIsisStatus
```

ip isis admin-state

Enables or disables the administrative status of IS-IS on the switch.

ip isis admin-state {enable | disable}

Syntax Definitions

enable	Enables IS-IS.
disable	Disables IS-IS.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

When IS-IS status is disabled, the configuration settings and related statistics of the protocol remain unaffected.

Examples

```
-> ip isis admin-state enable
-> ip isis admin-state disable
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
isisSysTable
   isisSysAdminState
```

ip isis area-id

Configures the area ID for the switch.

ip isis area-id *area address*

no ip isis area-id *area address*

Syntax Definitions

area address	A 1–13 byte variable length integer, which specifies the area address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the area ID.
- The area ID is part of the Network Service Access Point (NSAP) address.
- Other parts of NSAP address (system ID and selector ID) are not configurable. System ID is derived from router ID and selector ID remains always as 00.
- You can configure a maximum of three area addresses.

Examples

```
-> ip isis area-id 49.0001
-> no ip isis area-id 49.0001
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
isisManAreaAddrTable
   isisManAreaAddrExistState
```

ip isis level-capability

Configures the router level of the IS-IS protocol globally.

ip isis level-capability {level-1 | level-2 | level-1/2}

Syntax Definitions

level-1	Specifies that the router can operate at Level-1 only.
level-2	Specifies that the router can operate at Level-2 only.
level-1/2	Specifies that the router can operate at both Level-1 and Level-2.

Defaults

parameter	default
level-1 | level-2 | level-1/2	**level-1/2**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Changing the level capability restarts the IS-IS protocol.
- Configuring the level capability at the IS-IS circuit level is also possible.

Examples

```
-> ip isis level-capability level-1
-> ip isis level-capability level-2
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis vlan level-capability	Configures the IS-IS level on the specified circuit.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
isisSysTable
   isisSysType
```

ip isis auth-check

Enables or disables authentication check for IS-IS PDUs.

ip isis auth-check {enable | disable}

Syntax Definitions

enable	Enables authentication check for IS-IS PDUs.
disable	Disables authentication check for IS-IS PDUs.

Defaults

By default, authentication check is enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- If enabled, IS-IS PDUs that fail to match either of the authentication type and key requirements are rejected.
- If disabled, the authentication PDUs are generated and the IS-IS PDUs are authenticated on receipt. An error message will be generated in case of a mismatch; but PDUs will not be rejected.

Examples

```
-> ip isis auth-check enable
-> ip isis auth-check disable
```

Release History

Release 7.3.3; command was introduced;

Related Commands

ip isis auth-type	Enables authentication and configures the authentication type of IS-IS protocol globally.
ip isis level auth-type	Enables authentication and configures the authentication types for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisAuthCheck
```

ip isis auth-type

Enables authentication and configures the authentication type of IS-IS protocol globally.

ip isis auth-type {simple {key *key* **| encrypt-key** *encrypt_key***} | md5 {key** *key* | **encrypt-key** *encrypt_key***} | key-chain** *key-chain-id* **| none}**

Syntax Definitions

simple	Simple authentication will be used.
md5	Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
key	Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
encrypt_key	The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
key-chain-id	The configured keychain ID.
none	No authentication will be used.

Defaults

parameter	default
simple | **md5** | **key-chain** | **none**	**none**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the *encrypt_key* parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this *key* parameter during the CLI configuration.
- If the *encrypt_key* parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.

- This command configures the authentication type of IS-IS protocol globally. These settings can be overridden at each level.
- By default, the authentication is disabled and no authentication type is configured.
- If a keychain is applied globally, the authentication algorithm of its active key will be used for adjacency formation with all peers. Use **ip isis auth-type none** to remove the keychain from IS-IS adjacency configurations.

Examples

```
-> ip isis auth-type simple key rachel
-> ip isis auth-type md5 encrypt-key 7a1e441a014b4030
-> ip isis auth-type key-chain 2
```

Release History

Release 7.3.3; command was introduced.
Release 8.4.1; **key-chain** parameter added.

Related Commands

ip isis level auth-type	Enables authentication and configures the authentication types for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisAuthType
   vRtrIsisAuthKey
   vRtrIsisAuthKeyChainId
```

ip isis csnp-auth

Enables or disables the authentication of Complete Sequence Number PDUs (CSNPs).

ip isis csnp-auth

no ip isis csnp-auth

Syntax Definitions

N/A

Defaults

CSNP authentication check is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to prevent the CSNP authentication.

Examples

```
-> ip isis csnp-auth
-> no ip isis csnp-auth
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis level csnp-auth	Configures CSNP authentication for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisCsnpAuthentication
```

ip isis hello-auth

Enables or disables the authentication of Hello PDUs globally.

ip isis hello-auth

no ip isis hello-auth

Syntax Definitions

N/A

Defaults

Authentication check of Hello PDUs is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to prevent the authentication of Hello packets.

Examples

```
-> ip isis hello-auth
-> no ip isis hello-auth
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis level hello-auth	Enables or disables the authentication of Hello PDUs for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisHelloAuthentication
```

ip isis psnp-auth

Enables or disables the authentication of Partial Sequence Number PDUs (PSNPs).

ip isis psnp-auth

no ip isis psnp-auth

Syntax Definitions

N/A

Defaults

PSNP authentication check is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to prevent the authentication of PSNP packets.

Examples

```
-> ip isis psnp-auth
-> no ip isis psnp-auth
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis level psnp-auth	Configures the PSNP authentication for specific IS-IS levels.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisPsnpAuthentication
```

ip isis lsp-lifetime

Configures the time interval for which Link State PDUs generated by a router are considered valid by other routers in the same domain.

ip isis lsp-lifetime *seconds*

no ip isis lsp-lifetime

Syntax Definitions

seconds	Validity interval in seconds.The valid range is 350–65535.

Defaults

parameter	default
seconds	1200

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to restore the default value.

Examples

```
-> ip isis lsp-lifetime 760
-> no ip isis lsp-lifetime
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis vlan lsp-pacing-interval	Configures the interval between IS-IS LSP PDUs sent from the specified circuit.
show ip isis status	Displays the IS-IS status.
show ip isis database	Displays IS-IS LSP database information of the adjacent routers.

MIB Objects

```
vRtrIsisTable
  vRtrIsisLspLifetime
```

ip isis lsp-wait

Configures the intervals between the first, second and subsequently generated LSPs.

ip isis lsp-wait {max-wait | initial-wait | second-wait} *seconds*

no ip isis lsp-wait {max-wait | initial-wait | second-wait}

Syntax Definitions

max-wait	Specifies the maximum interval between two successive LSPs, in seconds. The valid range is 1–120.
initial-wait	Specifies the initial LSP generation delay, in seconds. The valid range is 0–100.
second-wait	Specifies the time interval between the first and second generated LSPs, in seconds. The valid range is 1–100.
seconds	Specifies the time interval.

Defaults

parameter	default
seconds **(max-wait)**	5
seconds **(initial-wait)**	0
seconds **(second-wait)**	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- Successive LSPs are generated at increasing **second-wait** interval until a maximum value is reached.

Examples

```
-> ip isis lsp-wait max-wait 25
-> no ip isis lsp-wait initial-wait
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis vlan lsp-pacing-interval	Configures the interval between IS-IS LSP PDUs sent from the specified circuit.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisLspInitialWait
   vRtrIsisLspSecondWait
   vRtrIsisLspMaxWait
```

ip isis spf-wait

Configures the intervals between the first, second, and subsequent SPF calculations.

ip isis spf-wait {max-wait *seconds* **| initial-wait** *milliseconds*| **second-wait** *milliseconds***}**

no ip isis spf-wait {max-wait | initial-wait | second-wait}

Syntax Definitions

max-wait *seconds*	Specifies the maximum interval between two successive SPF calculations, in seconds. The valid range is 1–120 seconds.
initial-wait *milliseconds*	Specifies the initial SPF calculation delay, in milliseconds. The valid range is 10–100000 milliseconds.
second-wait *milliseconds*	Specifies the interval between first and second generated SPFs, in milliseconds. The valid range is 1–100000 milliseconds.

Defaults

parameter	default
max-wait *seconds*	10
initial-wait *milliseconds*	1000
second-wait *milliseconds*	1000

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- Successive SPF calculations are generated at exponentially increasing **second-wait** interval until a maximum value is reached.

Examples

```
-> ip isis spf-wait max-wait 25
-> no ip isis spf-wait initial-wait
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisSpfWait
   vRtrIsisSpfInitialWait
   vRtrIsisSpfSecondWait
```

ip isis summary-address

Adds or deletes the summary address.

ip isis summary-address {*ip_prefix/mask* **|** *ip_prefix* **[**/*netmask***]} {level-1 | level-2 | level-1/2}**

no ip isis summary-address {*ip_prefix/mask* **|** *ip_prefix* **[**/*netmask***]}**

Syntax Definitions

ip_prefix/mask	Specifies the IP prefix in dotted decimal notation and the mask length.
ip_prefix	Specifies the IP prefix in dotted decimal notation.
/netmask	Specifies the subnet mask in dotted decimal notation.
level-1	Specifies the IS-IS level as Level-1.
level-2	Specifies the IS-IS level as Level-2.
level-1/2	Specifies the IS-IS level as Level-1/2.

Defaults

parameter	default
level-1 | level-2 | level-1/2	**level-1/2**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an already configured summary address.
- Native IS-IS routes can only be summarized into Level-2 from the Level-1 database.
- It is not possible to summarize IS-IS internal routes at Level-1, although it is possible to summarize external (redistributed) routes at Level-1.
- IS-IS routes are not summarized by default.

Examples

```
-> ip isis summary-address 10.0.0.0/8 level-2
-> no ip isis summary-address 10.0.0.0/8
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis summary-address	Displays the IS-IS summary address database.

MIB Objects

```
vRtrIsisSummaryTable
   vRtrIsisSummRowStatus
```

ip isis overload

Enables and configures the IS-IS router to operate in the overload state for a specified time period.

ip isis overload [timeout *seconds***]**

no ip isis overload [timeout]

Syntax Definitions

timeout *seconds*	Specifies the timeout interval, in seconds. The valid range is 60–1800.

Defaults

By default, the IS-IS overload state is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to make the router exit the overload state.
- If the time period is not specified, the router remains in the overload state for an infinite period.
- During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is used only if the destination route is directly reachable by the router i.e., it will not be used for other transit traffic.
- This command can be used when the router is overloaded or before executing a shutdown command to divert traffic around the router.

Examples

```
-> ip isis overload timeout 70
-> no ip isis overload timeout
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis overload-on-boot	Configures the IS-IS router to be in the overload state during bootup for a specified time period.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
isisSysTable
   isisSysSetOverload
vRtrIsisTable
   vRtrIsisOverloadTimeout
```

ip isis overload-on-boot

Configures the IS-IS router to be in the overload state after bootup for a specified time period.

ip isis overload-on-boot [timeout *seconds***]**

no ip isis overload-on-boot [timeout *seconds***]**

Syntax Definitions

timeout *seconds*	Specifies the timeout interval, in seconds. The valid range is 60–1800.

Defaults

By default, the IS-IS router will not be in the overload state.

parameter	default
timeout *seconds*	60

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to prevent the router from entering the overload state after bootup.
- The router in the overload state is used only if there is no alternate path to reach the destination.
- This command configures the router after bootup in the overload state until the timeout timer expires or a timeout value is specified in the **no** form of this command.
- The **no overload** command does not influence the overload-on-boot function.

Examples

```
-> ip isis overload-on-boot timeout 80
-> no ip isis overload-on-boot timeout
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis overload	Sets the IS-IS router to operate in the overload state.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisOverloadOnBoot
   vRtrIsisOverloadOnBootTimeout
```

ip isis graceful-restart

Configures graceful restart of the router. It allows routing protocols to reconverge faster, minimizing service interruption.

ip isis graceful-restart

no ip isis graceful-restart

Syntax Definitions

N/A

Defaults

Graceful restart is disabled on the router by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable graceful restart and remove the graceful restart configuration from the IS-IS router.
- When graceful restart is enabled, the router can either be a helper (which helps a neighbor router to restart) or a restarting router, or both. In the current release, only the helper mode of a router is supported.

Examples

```
-> ip isis graceful-restart
-> no ip isis graceful-restart
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis graceful-restart helper	Configures the helper mode of routers for graceful restart.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisGracefulRestart
```

ip isis graceful-restart helper

Administratively enables and disables the IS-IS router to operate in the helper mode in response to a router performing a graceful restart.

ip isis graceful-restart helper {enable | disable}

Syntax Definitions

enable	Enables the helper mode on the router.
disable	Disables the helper mode on the router.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When graceful restart is enabled, the helper mode is enabled by default.
- When graceful restart helper is enabled on a router, it can help other restarting routers.

Examples

```
-> ip isis graceful-restart helper disable
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis graceful-restart	Configures graceful restart on the router.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisGRHelperMode
```

ip isis strict-adjacency-check

Enables or disables the adjacency check configuration on the router.

ip isis strict-adjacency-check {enable | disable}

Syntax Definitions

enable	Enables the adjacency check configuration on the router.
disable	Disables the adjacency check configuration on the router.

Defaults

By default, the adjacency check configuration is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the adjacency check configuration is enabled, both routers have to run the same IP version only in the IS-IS protocol to form an adjacency.
- When the adjacency check configuration is disabled, one common IP version running between two routers is enough to form an adjacency in the IS-IS protocol.

Examples

```
-> ip isis strict-adjacency-check enable
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisTable
   vRtrIsisStrictAdjacencyCheck
```

ip isis level auth-type

Enables authentication and configures the authentication types for specific IS-IS levels.

ip isis level {1 | 2} auth-type {simple {key *key* | **encrypt-key** *encrypt_key***} | md5 {key** *key* | **encrypt-key** *encrypt_key***} | key-chain** *key-chain-id* **| none}**

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
simple	Simple authentication will be used.
md5	Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
key	Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
encrypt_key	The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
key-chain-id	The configured keychain ID.
none	No authentication will be used.

Defaults

parameter	default
simple | **md5** | **key-chain** | **none**	**none**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
- Use the **key** parameter to configure the password for Simple or MD5 authentication. Alternatively, use the *encrypt_key* parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this *key* parameter during the CLI configuration.

- If the *encrypt_key* parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.
- This command overrides the global configuration of IS-IS authentication type.
- This command also sets the password or hash-key according to the type of authentication.
- Use **key-chain** parameter to apply a keychain to IS-IS adjacency at the capability level. Use **ip isis level auth-type none** to remove the capability level keychain authentication.
- By default, the authentication is disabled and no authentication type is configured.

Examples

```
-> ip isis level 2 auth-type simple key rachel
-> ip isis level 2 auth-type md5 encrypt-key 7a1e441a014b4030
-> ip isis level 2 auth-type key-chain 1
-> ip isis level 2 auth-type none
```

Release History

Release 7.3.3; command was introduced.
Release 8.4.1; **key-chain** parameter added.

Related Commands

ip isis auth-type	Enables authentication and configures the authentication type for the IS-IS protocol globally.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   vRtrIsisLevelAuthType
   vRtrIsisLevelAuthKey
   vRtrIsisLevel
   vRtrIsisLevelAuthKeyChainId
```

ip isis level hello-auth

Enables or disables the authentication of Hello PDUs for specific IS-IS levels.

ip isis level {1 | 2} hello-auth

no ip isis level {1 | 2} hello-auth

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

Authentication check of Level Hello PDUs is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to prevent the authentication of Hello packets at the specified IS-IS level.
- This command overrides the global configuration of IS-IS Hello authentication.

Examples

```
-> ip isis level 1 hello-auth
-> no ip isis level 1 hello-auth
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis hello-auth	Enables or disables the authentication of Hello PDUs globally.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   vRtrIsisLevelHelloAuthentication
```

ip isis level csnp-auth

Enables or disables the CSNP authentication for specific IS-IS levels.

ip isis level {1 | 2} csnp-auth

no ip isis level {1 | 2} csnp-auth

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

CSNP authentication check for specific IS-IS levels is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to prevent the authentication of CSNPs at the specified IS-IS level.
- This command overrides the global configuration of IS-IS CSNP authentication.

Examples

```
-> ip isis level 1 csnp-auth
-> no ip isis level 1 csnp-auth
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis csnp-auth	Enables or disables the authentication of CSNPs.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   vRtrIsisLevelCsnpAuthentication
```

ip isis level psnp-auth

Enables or disables PSNP authentication for specific IS-IS levels.

ip isis level {1 | 2} psnp-auth

no ip isis level {1 | 2} psnp-auth

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

PSNP authentication check for specific IS-IS levels is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to prevent the authentication of PSNPs at the specified IS-IS level.
- This command overrides the global configuration of IS-IS PSNP authentication.

Examples

```
-> ip isis level 1 psnp-auth
-> no ip isis level 1 psnp-auth
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis psnp-auth	Enables or disables the authentication of PSNPs.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   vRtrIsisLevelPsnpAuthentication
```

ip isis level wide-metrics-only

Enables the wide metrics in LSPs for specific IS-IS levels.

ip isis level {1 | 2} wide-metrics-only

no ip isis level {1 | 2} wide-metrics-only

Syntax Definitions

1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

By default, wide metrics is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the narrow metric (1–63).
- Wide metrics are used for improved granularity of metrics.
- Numeric values above 63 indicate wide metrics.

Examples

```
-> ip isis level 1 wide-metrics-only
-> no ip isis level 1 wide-metrics-only
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisLevelTable
   VrtrIsisLevelWideMetricsOnly
```

ip isis activate-ipv6|ipv4

Configures the IPv6 or IPv4 routing in IS-IS.

ip isis {activate-ipv6 | activate-ipv4}

no ip isis {activate-ipv6 | activate-ipv4}

Syntax Definitions

activate-ipv6	Enables IPv6 routing in IS-IS.
activate-ipv4	Enables IPv4 routing in IS-IS.

Defaults

By default, both IPv4 and IPv6 routing is enabled in IS-IS.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The **no** form of this command disables the IPv4/IPv6 routing in IS-IS.

Examples

```
-> ip isis activate-ipv6
-> ip isis activate-ipv4
-> no ip isis activate-ipv4
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisActivateIPV4
vRtrIsisActivateIPV6
```

ip isis vlan

Configures IPv4 or IPv6 IS-IS circuit on a particular VLAN. This command enables IS-IS routing on a particular VLAN. This is used to add both the IPv4 and IPv6 interfaces on a particular VLAN to the IS-IS circuit.

ip isis vlan *vlan_id* **[address-family {v4 | v6 | v4v6}]**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN on which IS-IS is to be enabled.
v4 | v6 | v4v6	The address family extension. The type of interface (IPv4 or IPv6) is controlled by the address-family extension.

Defaults

By default, both address families (IPv4 and IPv6) are disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The **no** form of this command disables IPv4/IPv6 IS-IS circuit on a particular VLAN.

Examples

```
-> ip isis vlan 10
-> ip isis vlan 10 address-family v6
-> no ip isis vlan 10 address-family v6
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisIfRowStatus
```

ip isis vlan admin-state

Enables or disables IS-IS on a circuit.

ip isis vlan *vlan_id* **admin-state {enable | disable}**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN on which IS-IS routing is to be enabled.
enable	Administratively enables IS-IS on the VLAN.
disable	Administratively disables IS-IS on the VLAN.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

When the status is manually disabled, the configuration settings and related statistics of the protocol remain unaffected.

Examples

```
-> ip isis vlan 10 admin-state enable
-> ip isis vlan 10 admin-state disable
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
isisCircTable
   isisCircAdminState
```

ip isis vlan interface-type

Configures the IS-IS interface (circuit) type as broadcast or point-to-point.

ip isis vlan *vlan_id* **interface-type {broadcast | point-to-point}**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
broadcast	Sets the interface (circuit) type as a broadcast IS-IS interface.
point-to-point	Sets the interface (circuit) type as a point-to-point IS-IS interface.

Defaults

parameter	default
broadcast | point-to-point	**broadcast**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ip isis vlan 10 interface-type broadcast
-> ip isis vlan 10 interface-type point-to-point
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis vlan default-type	Sets the interface type to default, that is, broadcast.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
isisCircTable
   isisCircType
```

ip isis vlan csnp-interval

Configures the time interval in seconds to send Complete Sequence Number PDUs (CSNP) PDUs from the specified VLAN circuit.

ip isis vlan *vlan_id* **csnp-interval** *seconds*

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
seconds	The time interval in seconds between successive CSNP PDUs sent on an interface after which IS-IS must generate a CSNP PDU on the specified circuit. The valid range is 1–65535.

Defaults

parameter	default
seconds	Broadcast interface: 10 seconds Point-to-Point interface: 5 seconds

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The **no** form of this command reverts the time interval to the default value.

Examples

```
-> ip isis vlan 10 csnp-interval 10
-> no ip isis vlan 10 csnp-interval
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisIfCsnpInterval
```

ip isis vlan hello-auth-type

Configures the authentication settings for the hello protocol at a circuit level.

ip isis vlan *vlan_id* **hello-auth-type {simple {key** *key* **| encrypt-key** *encrypt_key***} | md5 {key** *key* **| encrypt-key** *encrypt_key***} | key-chain** *key-chain-id* **| none}**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
simple	Simple authentication will be used.
md5	Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
key	Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
encrypt_key	The key in hexadecimal format to provide security considerations on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
key-chain-id	The configured keychain ID.
none	No authentication will be used.

Defaults

parameter	default
simple | **md5** | **key-chain** | **none**	**none**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the *encrypt_key* parameter to configure the password by supplying the encrypted form of the password as the encrypt_key. The Configuration snapshot always displays the password in the encrypted form. You must use only this *key* parameter during the CLI configuration.
- If the *encrypt_key* parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt_key.

- Use **key-chain** parameter to apply a keychain at a circuit level. Use **ip isis vlan hello-auth-type none** to remove the circuit level keychain authentication.
- By default, the authentication is disabled and no authentication type is configured.

Examples

```
-> ip isis vlan 10 hello-auth-type md5 key asddfgfhno
-> ip isis vlan 10 hello-auth-type simple key sdsdff
-> ip isis vlan 100 hello-auth-type key-chain 1
-> ip isis vlan 100 hello-auth-type none
```

Release History

Release 7.3.3; command was introduced.
Release 8.4.1; **key-chain** parameter added.

Related Commands

ip isis vlan level hello-auth-type	Configures the authentication of Hello PDUs for the specified IS-IS level of an IS-IS Circuit.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfHelloAuthKey
vRtrIsisIfHelloAuthType
vRtrIsisIfHelloAuthKeyChainId
```

ip isis vlan level-capability

Configures the IS-IS level on the specified circuit.

ip isis vlan *vlan_id* **level-capability [level-1 | level-2 | level-1/2]**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
level-1	Specifies that the interface can operate at Level-1 only.
level-2	Specifies that the interface can operate at Level-2 only.
level-1/2	Specifies that the interface can operate at both Level-1 and Level-2.

Defaults

parameter	default
level-1 | **level-2** | **level-1/2**	**level-1/2**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Changing the level capability restarts the IS-IS protocol on the interface.
- If the level capability is configured globally and on a specific interface, the combination of the two settings will decide the potential adjacency.

Examples

```
-> ip isis vlan 10 level-capability level-1
-> ip isis vlan 10 level-capability level-1/2
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis level-capability	Configures the router level of the IS-IS protocol globally.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
isisCircTable
   isisCircLevel
```

ip isis vlan lsp-pacing-interval

Configures the interval between IS-IS LSP PDUs sent from the specified circuit.

ip isis vlan *vlan_id* **lsp-pacing-interval** *milliseconds*

no ip isis vlan *vlan_id* **lsp-pacing-interval**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
milliseconds	The time interval in milliseconds (from 0 to 65535) between IS-IS LSPs.

Defaults

parameter	default
milliseconds	100

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the default settings.
- No LSPs are sent from the specified interface if the time interval is set to 0.

Examples

```
-> ip isis vlan 10 lsp-pacing-interval 1000
-> no ip isis vlan 10 lsp-pacing-interval
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis lsp-lifetime	Configures the time interval for which LSPs generated by a router is considered valid by other routers in the same domain.
ip isis lsp-wait	Configures the time interval between successively generated LSPs.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisIfLspPacingInterval
```

ip isis vlan passive

Configures the IS-IS circuit as passive.

ip isis vlan *vlan_id* **passive**

no ip isis vlan *vlan_id* **passive**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.

Defaults

By default, the interface is not passive.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the passive attribute.
- This command adds the passive attribute that causes the IS-IS circuit to be advertised as an IS-IS circuit without running the IS-IS protocol. Normally, only interface addresses that are configured for IS-IS are advertised as IS-IS interface at the level that they are configured. When the passive mode is enabled, the interface or the interface at the level ignores ingress IS-IS PDUs (Protocol Data Unit) and will not transmit IS-IS protocol PDUs.

Examples

```
-> ip isis vlan 10 passive
-> no ip isis vlan 10 passive
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis vlan level passive	Configures the IS-IS circuit as passive at the specified IS-IS level.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
isisCircTable
   isisCircPassiveCircuit
```

ip isis vlan retransmit-interval

Configures the minimum time interval between LSP (Link State Packet) retransmissions on a point-to-point interface.

ip isis vlan *vlan_id* **retransmit-interval** *seconds*

no ip isis vlan *vlan_id* **retransmit-interval**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
seconds	The minimum time interval (1–65535) in seconds between LSP transmissions on a point-to-point interface.

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the default settings.
- The retransmit interval should be greater than the expected round-trip delay between two devices to avoid any needless retransmission of PDUs.

Examples

```
-> ip isis vlan 10 retransmit-interval 130
-> no ip isis vlan 10 retransmit-interval
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfTbale
   vRtrIsisIfRetransmitInterval
```

ip isis vlan default-type

Sets the interface type to default, that is, broadcast.

ip isis vlan *vlan_id* **default-type**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ip isis vlan 10 default-type
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis vlan interface-type	Configures the IS-IS interface (circuit) type as broadcast or point-to-point.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisIfTypeDefault
```

ip isis vlan level hello-auth-type

Configures the authentication of Hello PDUs for the specified IS-IS level of an IS-IS Circuit.

ip isis vlan *vlan_id* **level {1 | 2} hello-auth-type {simple {key** *key* | **encrypt-key** *encrypt_key***} | md5 {key** *key* **| encrypt-key** *encrypt_key***} | key-chain** *key-chain-id* **| none}**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
simple	Simple authentication will be used.
md5	Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
key	Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
encrypt_key	The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
key-chain-id	The configured keychain ID.
none	No authentication will be used.

Defaults

parameter	default
simple | **md5** | **key-chain** | **none**	**none**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the *encrypt_key* parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this *key* parameter during the CLI configuration.

- If the *encrypt_key* parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.
- This command also configures the authentication type and the corresponding key. These settings override the configuration done at an interface level.
- Use **key-chain** parameter to apply a keychain at the capability level per circuit. Use **ip isis vlan level hello-auth-type none** to remove the capability level keychain authentication per circuit.
- By default, the authentication is disabled and no authentication type is configured.

Examples

```
-> ip isis vlan 10 level 1 hello-auth-type md5 key xyz123
-> ip isis vlan 10 level 2 hello-auth-type none
-> ip isis vlan 100 level 2 hello-auth-type key-chain 1
-> ip isis vlan 100 level 2 hello-auth-type none
```

Release History

Release 7.3.3; command was introduced.
Release 8.4.1; **key-chain** parameter added.

Related Commands

ip isis vlan hello-auth-type	Configures the authentication settings for the hello protocol at a circuit level.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelHelloAuthType
   vRtrIsisIfLevelHelloAuthKey
   vRtrIsisIfLevel
   vRtrIsisIfLevelHelloAuthKeyChainId
```

ip isis vlan level hello-interval

Configures the time interval between the successive Hello PDUs for the specified IS-IS level on a circuit.

ip isis vlan *vlan_id* **level {1 | 2} hello-interval** *seconds*

no ip isis vlan *vlan_id* **level {1 | 2} hello-interval**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
seconds	The hello interval, in seconds. The valid range is 1–20000.

Defaults

parameter	default
seconds (designated routers)	3
seconds (non-designated routers)	9

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to restore the default settings.

Examples

```
-> ip isis vlan 10 level 1 hello-interval 50
-> no isis vlan 10 level 2 hello-interval
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelHelloTimer
```

ip isis vlan level hello-multiplier

Configures the number of missing Hello PDUs from a neighbor, after which the adjacency is declared as down.

ip isis vlan *vlan_id* **level {1 | 2} hello-multiplier** *number*

no ip isis vlan *vlan_id* **level {1 | 2} hello-multiplier**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
number	The multiplier (2–100) of the hello interval.

Defaults

parameter	default
number	3

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to restore the default settings.

Examples

```
-> ip isis vlan 10 level 1 hello-multiplier 10
-> no ip isis vlan 10 level 2 hello-multiplier
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
isisCircLevelTable
   isisCircLevelHelloMultiplier
```

ip isis vlan level metric

Configures the metric value of the specified IS-IS level of the circuit.

ip isis vlan *vlan_id* **level {1 | 2} metric** *number*

no ip isis vlan *vlan_id* **level {1 | 2} metric**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
number	The metric value (1–16777215) assigned for the specified level of the circuit.

Defaults

parameter	default
number	10

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- To calculate the lowest cost to reach a destination, each configured level on each circuit must have a cost. The costs for each level on a circuit may be different. If the metric is not configured, the default of 10 is used.

Examples

```
-> ip isis vlan 10 level 1 metric 25
-> no ip isis vlan 10 level 2 metric
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelAdminMetric
```

ip isis vlan level passive

Configures the IS-IS circuit as passive at the specified IS-IS level.

ip isis vlan *vlan_id* **level {1 | 2} passive**

no ip isis vlan *vlan_id* **level {1 | 2} passive**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.

Defaults

By default, the interface level passive configuration is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the passive attribute.
- This command adds the passive attribute that causes the IS-IS circuit at the given level to be advertised as an IS-IS circuit without running the IS-IS protocol. Normally, only interface addresses that are configured for IS-IS are advertised as IS-IS interface at the level that they are configured. When the passive mode is enabled, the interface or the interface at the level ignores ingress IS-IS protocol PDUs and will not transmit IS-IS protocol PDUs.

Examples

```
-> ip isis vlan 10 level 1 passive
-> no ip isis vlan 10 level 1 passive
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis vlan passive	Configures the IS-IS circuit as passive.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelPassive
```

ip isis vlan level priority

Configures the priority of the IS-IS circuit for the designated router election on a multi-access network.

ip isis vlan *vlan_id* **level [1 | 2] priority** *number*

no ip isis vlan *vlan_id* **level [1 | 2] priority**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
1	Specifies the IS-IS level as Level-1.
2	Specifies the IS-IS level as Level-2.
number	The priority value of the IS-IS circuit at this level. The valid range is 0–127.

Defaults

parameter	default
number	64

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- This priority is included in hello PDUs transmitted by the circuit on a multi-access network.
- The router with the highest priority is the preferred designated router.
- The designated router sends LSPs to this network and also to the routers that are attached to it.

Examples

```
-> ip isis vlan 10 level 1 priority 4
-> ip isis vlan 10 level 2 priority 4
-> no ip isis vlan 10 level 1 priority
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfLevelTable
   vRtrIsisIfLevelISPriority
```

ip isis summary-address6

Configures the IPv6 summary address.

ip isis summary-address6 {*ipv6_prefix/prefix_length* **|** *ipv6_address***} {level-1 | level-2 | level-1/2}**

no ip isis summary-address6 {*ipv6_prefix/prefix_length* **|** *ipv6_address***} {level-1 | level-2 | level-1/2}**

Syntax Definitions

ipv6_prefix/prefix_length	IPv6 prefix and prefix length.
ipv6_address	IPv6 address.
level-1	Specifies that the routes can be summarized at Level-1 only.
level-2	Specifies that the routes can be summarized at Level-2 only.
level-1/2	Specifies that the routes can be summarized at both Level-1 and Level-2.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove an already configured summary address.

Examples

```
-> ip isis summary-address6 4001::/16 level-1
-> no ip isis summary-address6 4001::/16
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis summary-address6 Displays the IS-IS IPv6 summary address database.

MIB Objects

```
vRtrIsisInetSummLevel
vRtrIsisInetSummRowStatus
```

ip isis bfd-state

Enables or disables the registration of IS-IS with the BFD protocol.

ip isis bfd-state {enable | disable}

Syntax Definitions

enable	Enables BFD for IS-IS.
disable	Disables BFD for IS-IS.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- BFD must be globally enabled for the switch and IS-IS must be registered with BFD at the protocol level before IS-IS can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and IS-IS acts based upon the BFD message.
- Whenever a neighbor goes down, IS-IS will inform BFD to remove that neighbor from the BFD active list.

Examples

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of IS-IS with the BFD protocol:

```
-> ip isis bfd-state enable
-> ip isis bfd-state disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ip bfd admin-state	Enables or disables the global BFD protocol status for the switch.
ip isis bfd-state all-vlans	Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.
ip isis vlan bfd-state	Enables or disables BFD monitoring on a specific PIM interface.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisBfdStatus
```

ip isis bfd-state all-vlans

Enables or disables BFD monitoring for all IS-IS VLANs in the switch configuration.

ip isis bfd-state all-vlans {enable | disable}

Syntax Definitions

enable	Enables BFD for all the IS-IS VLANs.
disable	Disables BFD for all the IS-IS VLANs.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for IS-IS must be enabled before IS-IS can interact with BFD.

Examples

```
-> ip isis bfd-state all-vlans enable
-> ip isis bfd-state all-vlans disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ip isis bfd-state	Enables or disables the registration of IS-IS with the BFD protocol.
ip isis vlan bfd-state	Enables or disables BFD monitoring on a specific IS-IS VLAN.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisTable
   vRtrIsisBfdAllVlanStatus
```

ip isis vlan bfd-state

Enables or disables BFD monitoring for a specific IS-IS VLAN.

ip isis vlan *vlan_id* **bfd-state {enable | disable}**

Syntax Definitions

vlan_id	The VLAN ID of a given VLAN.
enable	Enables BFD for the specified IS-IS VLAN.
disable	Disables BFD for the specified IS-IS VLAN.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Registering IS-IS with BFD is required at the protocol level before IS-IS can interact with BFD.
- When BFD is enabled on the specified IS-IS VLAN, BFD is applied to all IPv4 and IPv6 interfaces configured for the VLAN.
- A single IS-IS adjacency covers both IPv4 and IPv6 interfaces, but the interfaces are treated independently within the adjacency. If an IS-IS adjacency has both interface types, there will be two BFD sessions (one for each interface). When one interface goes down, only the routes learned through that interface are removed.

Examples

```
-> ip isis vlan 10 bfd-state enable
-> ip isis vlan 10 bfd-state disable
```

Release History

Release 8.4.3.R03; command was introduced.

Related Commands

ip isis bfd-state	Enables or disables the registration of IS-IS with the BFD protocol.
ip isis bfd-state all-vlans	Enables or disables BFD monitoring for all IS-IS interfaces in the switch configuration.
show ip isis vlan	Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

```
vRtrIsisIfTable
   vRtrIsisIfBfdStatus
```

show ip isis adjacency

Displays information about IS-IS adjacent routers.

show ip isis adjacency [{system-id *nbr_sys_id* **| vlan** *vlan_id***}] [detail]**

Syntax Definitions

nbr_sys_id	The system ID of the neighbor router.
vlan_id	The VLAN ID of a given VLAN.

Defaults

By default adjacency information for all the neighbor routers are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use *the nbr_sys_id* or *vlan_id* parameter with this command to view the adjacency information for a specific neighbor.

Examples

```
-> show ip isis adjacency
================================================================================
ISIS Adjacency
================================================================================
System ID          Type     State    Hold       VlanID    MT IDs    Hostname
--------------------------------------------------------------------------------
0000.0000.0001     L1        UP        25        20       0, 2      Router-A
0000.0000.0002     L2        UP        21        30       None      Router-B
--------------------------------------------------------------------------------
Adjacency : 2
================================================================================
```

output definitions

System ID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
Type	The level (**LI, L2,** or **L1/L2**) of the adjacent router.
State	The state of the adjacent router (**Up** or **Down**).
Hold	The Hold time of the adjacent router.
VlanID	The VLAN ID of the adjacent router.
MT IDs	MT IDs sent by MT enabled ISIS neighbour. '0' signifies the IPv4 support, '2' signifies IPv6 support, 'none' signifies MT disabled neighbour.

output definitions

Hostname	The host name of the adjacent router.
Adjacencies	The total number of adjacent routers.

```
-> show ip isis adjacency detail
================================================================================
ISIS adjacency
================================================================================
--------------------------------------------------------------------------------
SystemID     : 0000.0000.0001       SNPA       : 00:d0:95:f3:0f:08
VlAN         : 20                   Up Time    : WED JUN 05 05:18:51 2013
State        : UP                   Priority   : 64
Nbr Sys Type : L2                   L.CircType : L1L2
Hold Time    : 6                    Max Hold   : 9
Adj Level    : L2                   Host-name  : Router-A
MT IDs       : 0, 2                 NLPIDs     : IPv4, IPv6
IPv4 Neighbor      : 2.2.2.3
Ipv6 Neighbor      : FE80::C809:FFF:FEDC:0
Restart Support    : Disabled
Restart Status     : Not currently being helped
Restart Suppressed : Disabled

--------------------------------------------------------------------------------
SystemID     : 0000.0000.0002       SNPA       : 00:d0:95:f3:0f:08
VlAN         : 10                   Up Time    : WED JUN 05 05:18:51 2013
State        : UP                   Priority   : 64
Nbr Sys Type : L1                   L.CircType : L1L2
Hold Time    : 6                    Max Hold   : 9
Adj Level    : L2                   Host-name  : Router-B
MT IDs       : None                 NLPIDs     : IPv4
IPv4 Neighbor      : 2.2.2.3
Ipv6 Neighbor      : FE80::C809:AFF:FEEC:0
Restart Support    : Disabled
Restart Status     : Not currently being helped
Restart Suppressed : Disabled
--------------------------------------------------------------------------------
Adjacency : 2
================================================================================
```

output definitions

SystemID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
VLAN	The Vlan ID in which the adjacency is present.
MT IDs	MT IDs sent by MT enabled ISIS neighbor. '0' signifies the IPv4 support, '2' signifies IPv6 support, 'none' signifies MT disabled neighbor.
NLPIDs	The IP address families supported by IS-IS neighbor: IPv4 or IPv6
State	The state of the adjacent router (**Up** or **Down**).
Adj Level	The adjacency level (**L1** or **L2**) of the router.
Nbr Sys Type	The type of the neighboring router(**L1, L2** or **L1L2**)
Hold Time	The Hold time of the adjacent router.

output definitions

IPv4 Neighbor	The 32-bit IP address of the neighbor.
IPv6 Neighbor	The 32-bit IPv6 address of the neighbor
Restart Support	Indicates if graceful restart is **enabled** or **disabled**.
Restart Status	Indicates whether the router is currently helping an adjacent router to restart.
Restart Suppressed	Indicates whether the advertisement of LSPs are suppressed (**enabled**) or not (**disabled**) as per the request of adjacent router.
SNPA	The SNPA address of the adjacent router.
Up Time	Indicates the time period in seconds, during which the router was in the adjacency.
Priority	The priority of the adjacent router.
Host-name	The host name of the adjacent router.
L. CircType	Indicates the level circuit type (**L1, L2** or **L1L2**) of the adjacent router.
Max Hold	Indicates the maximum Hold time of the adjacent router.

Release History

Release 7.3.3; command was introduced.

Related Commands

clear ip isis adjacency	Clears and resets the IS-IS adjacency database.

MIB Objects

```
isisISAdjTable
   isisISAdjIndex
   isisISAdjState
   isisISAdjNeighSNPAAddress
   isisISAdjNeighSysType
   isisISAdjNeighSysID
   isisISAdjUsage
   isisISAdjNeighPriority
   isisISAdjUpTime
   isisISAdjHoldTimer
vRtrIisisISAdjTable
   vRtrIsisISAdjCircLevel
   vRtrIsisISAdjRestartSupport
   vRtrIsisISAdjRestartSupressed
   vRtrIsisISAdjExpireIn
   vRtrIsisISAdjNeighborIP
   vRtrIsisISAdjRestartStatus
   vRtrIsisISAdjMTIdMask
```

show ip isis database

Displays IS-IS LSP database information of the adjacent routers.

show ip isis database [{system_id *system_id* **| lsp_id** *lsp_id***}] [detail] [level {1 | 2}]**

Syntax Definitions

system_id	The system ID of the router.
lsp_id	The LSP ID.
detail	Indicates that the output is displayed in a detailed manner.
level	Indicates the IS-IS level, either **1** or **2**.

Defaults

By default, the entire LSP database is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use *system_id* or *lsp_id* parameter with this command to view specific LSP database information.
- Use the **level** parameter with this command to view the LSP database information of a particular level.

Examples

```
-> show ip isis database
Legends : P            =  The Partition repair bit is set
OV    = The overload bit is set
ATT   = The Attach bit is set
L1    = Specifies a Level 1 IS type
L2    = Specifies a Level 2 IS type
=================================================================
ISIS Database
=================================================================
LSP ID                    Sequence  Checksum  Lifetime  Attributes
-----------------------------------------------------------------
Displaying level-1 database
-----------------------------------------------------------------
1720.2116.0051.00-00      0x44      0xb664    919          L1L2
level-1 LSP count : 1

Displaying level-2 database
-----------------------------------------------------------------
1720.2116.0051.00-00      0x45      0xb465    1083         L1L2
level-2 LSP count : 1
=================================================================
```

output definitions

LSP ID	The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.
Sequence	The sequence number of the LSP. The sequence number is a value used to identify old and duplicate LSPs.
Checksum	The checksum value of the LSP.
Lifetime	The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the Link State Database of all the routers.
Attributes	The level capability of the router.
LSP Count	The number of LSPs in the Link State Database.

```
-> show ip isis database detail
   Legends : P    =  The Partition repair bit is set
             OV   =  The overload bit is set
             ATT  =  The Attach bit is set
             L1   =  Specifies a Level 1 IS type
             L2   =  Specifies a Level 2 IS type
=========================================================================
ISIS Database
=========================================================================
Displaying level-1 database
-------------------------------------------------------------------------
LSP ID        : 1720.2116.0051.00-00            Level     : L1
Sequence      : 0x44       Checksum  : 0xb664   Lifetime  : 818
Version       : 1          Pkt Type  : 18       Pkt Ver   : 1
Attributes    : L1L2       Max Area  : 3
SysID Len     : 6          Used Len  : 635      Alloc Len : 1489

TLVs  :
Area Addresses      :
   Area Address     :  (3)  49.0000
Supp protocols      :
   Protocols        :  Ipv4 , Ipv6
IS-Hostname         :
   Hostname         :  HostA
IS Neighbors        :
   Virtual Flag     :  0
   Neighbor         :  1720.2116.0052.00  Metric : 10 (I)
IPv4 I/F Address    :
   IP Address       : 172.21.160.51
   IP Address      : 172.21.160.52
IPv6 I/F Address    :
   IPv6 Address     : 2001:1::1
   IPv6 Address     : 3001:1::1
IPv4 Internal Reach :
   IP Prefix        : 16.16.16.0/24 (Dir.: UP )   Metric  : 10 (I)
   IP Prefix        : 17.17.17.0/24 (Dir.: UP )   Metric  : 10 (I)
IPv4 External Reach :
   IP Prefix        : 24.24.24.0/24 (Dir.: UP )   Metric  : 10 (E)
   IP Prefix        : 25.25.25.0/24 (Dir.: UP )   Metric  : 10 (E)
IPv6 Reach.         :
   IPv6 Prefix      : 2001:1::/64
                      Flags : Up Internal Metric : 10
   IPv6 Prefix      : 3001:1::/64
```

```
                      Flags : Up Internal Metric : 10
   IPv6 Prefix      : 4001:1::/64
                      Flags : Up Internal Metric : 10
TE IP Reach.        :
   IPv4 Prefix      : 11.1.1.0/24 (Dir.:Up)  Metric : 10
   IPv4 Prefix      : 22.1.1.0/24 (Dir.:Up)  Metric : 10
   IPv4 Prefix      : 21.1.1.0/24 (Dir.:Up)  Metric : 10
   IPv4 Prefix      : 10.135.38.0/24 (Dir.:Up)  Metric : 1

level-1 LSP count : 1

Displaying level-2 database
----------------------------------------------------------------
LSP ID        : 1720.2116.0051.00-00             Level     : L2
Sequence      : 0x45       Checksum  : 0xb465    Lifetime  : 981
Version       : 1          Pkt Type  : 20        Pkt Ver   : 1
Attributes    : L1L2       Max Area  : 3
SysID Len     : 6          Used Len  : 635       Alloc Len : 1489

TLVs  :
Area Addresses      :
   Area Address     :  (3) 49.0000
Supp protocols      :
   Protocols        :  Ipv4  Ipv6
IS-Hostname         :
   Hostname         :  HostA
IS Neighbors        :
   Virtual Flag     :  0
   Neighbor         :  1720.2116.0052.00  Metric : 10 (I)
IPv4 I/F Address    :
   IP Address       : 172.21.160.51
   IP Address       : 172.21.160.52
IPv6 I/F Address    :
   IPv6 Address     : 2001:1::1
   IPv6 Address     : 3001:1::1
IPv4 Internal Reach :
   IP Prefix        : 16.16.16.0/24 (Dir.: UP )   Metric  : 10 (I)
   IP Prefix        : 17.17.17.0/24 (Dir.: UP )   Metric  : 10 (I)
IPv4 External Reach :
   IP Prefix        : 24.24.24.0/24 (Dir.: UP )   Metric  : 10 (E)
   IP Prefix        : 25.25.25.0/24 (Dir.: UP )   Metric  : 10 (E)
IPv6 Reach.         :
   IPv6 Prefix      : 3001:1::/64
                      Flags : Up Internal Metric : 10
TE IP Reach.        :
   IPv4 Prefix      : 21.1.1.0/24 (Dir.:Up)  Metric : 10
   IPv4 Prefix      : 10.135.38.0/24 (Dir.:Up)  Metric : 1
   IPv4 Prefix      : 11.1.1.0/24 (Dir.:Up)  Metric : 1

level-2 LSP count : 1

================================================================
```

output definitions

LSP ID	The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.
Sequence	The sequence number of the LSP. The Sequence number is a value used to identify old and duplicate LSPs.
Checksum	The checksum value of the LSP.
Lifetime	The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the Link State Database of all the routers.
Version	The version of the IS-IS protocol that has generated the LSP.
Pkt Type	The IS-IS PDU type number derived from the PDU header, which can be **18** or **20**. The number 18 represents L1 LSP PDU type and 20 represents L2 LSP PDU type.
Pkt Ver	The version of the IS-IS protocol that has generated the packet.
Attributes	The level capability of the router.
Max Area	The Maximum number of areas supported by the originating router of the LSP.
SysID Len	The length of the system-id as used by the originating router.
Used Len	The length used by the LSP.
Alloc Len	The length allocated for the LSP to be stored.
Area Address	The area ID of the router.
Supp protocols	The network layer protocols that are supported.
IS-Host Name	The host name of the router.
System ID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
IS Neighbors	The list of reachable IS-IS neighbors.
IPv4 Internal Reach	The list of IS-IS internal routes.
IPv6 Reach	The list of IS-IS IPv6 internal routes.
IP Prefix	The IP address and subnet mask of the destination.
Metrics	The metric value to reach the destination.
IPv4 External Reach	The list of external IS-IS routes.
IPv6 Reach	The list of external IS-IS IPv6 routes.
level-1 LSP Count	The number of Level-1 LSPs.
level-2 LSP Count	The number of Level-2 LSPs.

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis hostname	Displays the database of IS-IS host name and its corresponding system ID.
clear ip isis lsp-database	Clears and resets the IS-IS LSP database information.

MIB Objects

```
vRtrIsisLSPTable
   vRtrIsisLSPId
   vRtrIsisLSPSeq
   vRtrIsisLSPChecksum
   vRtrIsisLSPLifetimeRemain
   vRtrIsisLSPAttributes
   vRtrisisLSPVersion
   vRtrIsisLSPPktType
   vRtrIsisLSPSysIdLen
   vRtrIsisLSPAllocLen
   vRtrIsisLSPMaxArea
   vRtrIsisLSPBuff
   vRtrisisLSPUsedLen
```

show ip isis hostname

Displays the database of IS-IS host name and its corresponding system ID.

show ip isis hostname

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip isis hostname
Hosts
================================================================================
System Id                     Hostname
--------------------------------------------------------------------------------
1800.0000.0002                core_west
1800.0000.0005                core_east
1800.0000.0008                asbr_west
1800.0000.0009                asbr_east
1800.0000.0010                abr_sjc
1800.0000.0011                abr_lax
1800.0000.0012                abr_nyc
1800.0000.0013                abr_dfw
1800.0000.0015                dist_oak
1800.0000.0018                dist_nj
1800.0000.0020                acc_nj
1800.0000.0021                acc_ri
1800.0000.0027                dist_arl
1800.0000.0028                dist_msq
1800.0000.0029                acc_arl
```

output definitions

System Id	The system ID of the router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-Octet hexadecimal system ID.
Hostname	The host name of the router.

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis adjacency	Displays information about IS-IS adjacent routers.
show ip isis database	Displays IS-IS LSP database information of the adjacent routers.
ip isis area-id	Configures the area ID for the router.

MIB Objects

```
vRtrIsisHostnameTable
   vRtrIsisSysID
   vRtrIsisHostname
```

show ip isis routes

Displays the IS-IS route information from the routing table.

show ip isis routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip isis routes
================================================================================
ISIS Routes
================================================================================
Prefix              Metric        Lvl/Type   SPF-num  Nexthop    System ID
--------------------------------------------------------------------------------
1.1.1.0/24          10            1/Int       7       0.0.0.0    1720.2116.0051
2.2.2.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
3.3.3.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
4.4.4.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
5.5.5.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
6.6.6.0/24          10            1/Int       1       0.0.0.0    1720.2116.0051
--------------------------------------------------------------------------------
Routes : 8
================================================================================
```

output definitions

Prefix	The IP prefix and mask of the destination routes.
Metric	The cost to reach the destination route.
Lvl/Type	The level and route type of the routes.
SPF-num	The version of the SPF calculation used to select the route.
Nexthop	The Next Hop address to reach the destination.
System ID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis adjacency	Displays information about IS-IS adjacent routers.
show ip isis database	Displays IS-IS LSP database information of the adjacent routers.

MIB Objects

```
vRtrIsisRouteTable
   vRtrIsisRouteLevel
   vRtrIsisRouteSpfVersion
   vRtrIsisRouteType
   vRtrisisRouteDest
   vRtrIsisRouteNexthopIP
   vRtrIsisRouteNexthopSysID
   vRtrIsisRouteMetric
   vRtrIsisRouteMask
```

show ip isis routes6

Displays the IS-IS IPv6 route information from the routing table.

show ip isis routes6

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip isis routes6
================================================================================
ISISv6 Routes
================================================================================
Prefix         Metric  Lvl/Type  Vlan-Id  Nexthop                   System ID
--------------------------------------------------------------------------------
2001:1::/64    10      1/Int     6        ::                        0300.0100.1001
3001:1::/64    10      1/Int     11       ::                        0300.0100.1001
4001:1::/64    10      1/Int     6        ::                        0300.0100.1001
5001:1::/64    20      1/Int     6        fe80::213:c3ff:fe9a:2761  0000.0000.0001
--------------------------------------------------------------------------------
Routes : 4
================================================================================
```

output definitions

Prefix	The IP prefix and mask of the IPv6 destination routes.
Metric	The cost to reach the destination route.
Lvl/Type	The level and route type of the routes.
SPF-num	The version of the SPF calculation used to select the route.
Nexthop	The Next Hop address to reach the destination.
System ID	The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis adjacency	Displays information about IS-IS adjacent routers.
show ip isis database	Displays IS-IS LSP database information of the adjacent routers.

MIB Objects

N/A

show ip isis spf

Displays the IS-IS SPF calculation information.

show ip isis spf [detail]

Syntax Definitions

detail	Indicates that the output is displayed in a detailed manner.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The SPF path table is common for both IPv4 and IPv6.

Examples

```
-> show ip isis spf
============================================================
ISIS Path Table
============================================================
Node                   VlanId         Nexthop
------------------------------------------------------------
0000.0000.0001.00      6             0000.0000.0001
------------------------------------------------------------
SPF count: 1
============================================================================
```

output definitions

Node	The system ID of the routers.
VlanId	The VLAN ID.
Nexthop	The system ID of the Next Hop router.

```
-> show ip isis spf detail
============================================================================
ISIS Path Table
============================================================================
----------------------------------------------------------------------------
Node       : 0000.0000.0001.00      Metric   : 10
VlanId     : 6                      SNPA     : None
Nexthop  : 0000.0000.0001
------------------------------------------------------------
SPF count: 1
============================================================================
```

output definitions

Node	The system ID of the routers.
Metric	The metric value used for SPF calculations.
VlanId	The VLAN ID.
SNPA	The SNPA address of the router.
Nexthop	The system ID of the Next Hop router.
SPF count	The number of SPF calculations done by the router.

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis spf-log	Displays the IS-IS SPF log.
show ip isis status	Displays the IS-IS status.

MIB Objects

```
vRtrIsisPathTable
   vRtrIsisPathID
   vRtrIsisPathIfIndex
   vRtrIsisPathNHopSysID
   vRtrIsisPathMetric
   vRtrIsisPathSNPA
```

show ip isis spf-log

Displays the IS-IS SPF log.

show ip isis spf-log [detail]

Syntax Definitions

detail	Indicates that the output is displayed in a detailed manner.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the last 20 IS-IS SPF events.

Examples

```
-> show ip isis spf-log
ISIS SPFLog
================================================================================
When       Duration       L1-Nodes      L2-Nodes      Event-Count
--------------------------------------------------------------------------------
01/30/2005 11:01:54 <0.01s 1              1               3
--------------------------------------------------------------------------------
Log Entries : 1
```

output definitions

When	The date on which the SPF calculation was completed.
Duration	The time duration of the event.
L1-Nodes	The number of Level-1 nodes.
L2-Nodes	The number of Level-2 nodes.
Event-Count	The number of SPF calculations.
Log Entries	The total number of log entries.

```
-> show ip isis spf-log detail

================================================================================
ISIS SPFLog
================================================================================
SpfTimeStamp          :  SUN OCT 01 05:15:29 2006
spfRunTime            :  0
Spf Involved L1 Nodes :  69
Spf Involved L2 Nodes :  71
Spf Event-count       :  169
Last TriggeredLspId   :  0020.0200.2001.00-4a
```

```
Spf Trigger Reason    :  newAdjacency(0) ,lspExpired(8) ,lspChanged(10)
SpfTimeStamp          :  SUN OCT 01 05:15:46 2006
spfRunTime            :  0
Spf Involved L1 Nodes :  72
Spf Involved L2 Nodes :  72
Spf Event-count       :  227
Last TriggeredLspId   :  0020.0200.2001.00-4a
Spf Trigger Reason    :  newAdjacency(0) ,lspExpired(8) ,lspChanged(10)
--------------------------------------------------------------------------------
Log Entries : 2
================================================================================
```

output definitions

SpfTimeStamp	The timestamp when the SPF run started on the system.
spfRunTime	The time (in hundredths of a second) required to complete the SPF run.
Spf Involved L1 Nodes	The number of Level-1 nodes involved in the SPF calculation.
Spf Involved L1 Nodes	The number of Level-2 nodes involved in the SPF calculation.
Spf Event-count	The number of SPF events that triggered the SPF calculation.
Last TriggeredLspId	The LSP ID of the last LSP processed before the SPF run.
Spf trigger Reason	Indicates the reasons (**newAdjacency**, **lspExpired**, or **lspChanged**) for SPF calculations.
Log Entries	The number of SPF logs.

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis spf	Displays the IS-IS SPF calculation information.
clear ip isis spf-log	Clears and resets the IS-IS SPF log information.

MIB Objects

```
vRtrIsisSpfLogTable
   vRtrIsisSpfRunTime
   vRtrIsisSpfL1Nodes
   VRtrIsisSpfL2Nodes
   vRtrIsisSpfEventCount
   vRtrIsisSpfLastTriggerLSPId
   vRtrIsisSpfTriggerReason
```

show ip isis statistics

Displays the IS-IS statistics information.

show ip isis statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip isis statistics
=============================================================================
ISIS Statistics
=============================================================================
ISIS Instance             : 1                           SPF Runs         : 44
Purge Initiated           : 0                           LSP Regens       : 54
CSPF Statistics
Requests                  : 0                           Request Drops    : 0
Paths Found               : 0                           Paths Not Found  : 0
-----------------------------------------------------------------------------
PDU Type  Received  Processed  Dropped Sent       Retransmitted
-----------------------------------------------------------------------------
LSP       185         184       1       54         0
IIH       8382        8382      0       2796       0
CSNP      3352        352       0       0          0
PSNP      0           0         0       4          0
Unknown   0           0         0       0          0
```

output definitions

ISIS Instance	The number of IS-IS instances.
SPF Runs	The number of SPF calculations that have been performed.
Purge Initiated	The number of purges that the system initiated. A purge is initiated if the router decides that a link-state PDU must be removed from the database.
LSP Regens	The number of LSPs that have been regenerated. An LSP is regenerated when it nears the end of its lifetime and has not changed.
Requests	The number of CSNP requests received.

output definitions (continued)

Request Drops	The number of CSNP requests that are dropped.
Paths Found	The number of paths found.
Paths Not Found	The number of paths not found.
PDU Type	The type of PDU.
Received	The number of PDUs received since IS-IS started or since the statistics were set to zero.
Processed	The number of PDUs that are processed (number of PDUs received less the number dropped).
Dropped	The number of PDUs that are dropped.
Sent	The number of PDUs transmitted since IS-IS started or since the statistics were set to zero.
Retransmitted	The number of PDUs that are retransmitted.

Release History

Release 7.3.3; command was introduced.

Related Commands

clear ip isis statistics	Clears and resets the IS-IS statistics information.

MIB Objects

```
vRtrIsisStatsTable
   vRtrIsisSpfRuns
   vRtrIsisLSPRegenerations
   vRtrIsisInitiatedPurges
   vRtrIsisLSPRecd
   vRtrIsisLSPDrop
   vRtrIsisLSPSent
   vRtrIsisLSPRetrans
   vRtrIsisIIHRecd
   vRtrIsisIIHDrop
   vRtrIsisIIHSent
   vRtrIsisIIHRetrans
   vRtrIsisCSNPRecd
   vRtrIsisCSNPDrop
   vRtrIsisCSNPSent
   vRtrIsisCSNPRetrans
   vRtrIsisPSNPRecd
   vRtrIsisPSNPDrop
   vRtrIsisPSNPSent
   vRtrIsisPSNPRetrans
   vRtrIsisUnknownRecd
   vRtrIsisUnknownDrop
   vRtrIsisUnknownSent
   vRtrIsisUnknownRetrans
   vRtrIsisCSPFRequests
   vRtrIsisCSPFDroppedRequests
   vRtrIsisCSPFPathsFound
   vRtrIsisCSPFPathsNotFound
```

show ip isis status

Displays the IS-IS status.

show ip isis status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip isis status
================================================================================
ISIS Status
================================================================================
System Id             : 2cfa.a213.e402
Admin State           : DOWN
Protocols Enabled     : IPv4 IPv6
Last Enabled          : Mon Oct 30 06:58:41 2017
Level Capability      : L1L2
Authentication Check  : True
Authentication Type   : None
Graceful Restart      : Disabled
GR helper-mode        : Disabled
LSP Lifetime          : 1200
LSP Wait              : Max: 5 sec  Initial: 0 sec  Second: 1 sec
Adjacency Check       : Loose
L1 Auth Type          : None
L2 Auth Type          : None
L1 Wide Metrics-only  : Disabled
L2 Wide Metrics-only  : Disabled
L1 LSDB Overload      : Disabled
L2 LSDB Overload      : Disabled
L1 LSPs               : 0
L2 LSPs               : 0
Last SPF              : Mon Oct 30 06:58:41 2017
SPF Wait              : Max: 10000 ms  Initial: 1000 ms  Second: 1000 ms
Hello-Auth Check      : Enabled
Csnp-Auth Check       : Enabled
Psnp-Auth Check       : Enabled
L1 Hello-Auth Check   : Enabled
L1 Csnp-Auth Check    : Enabled
```

```
L1 Psnp-Auth Check    : Enabled
L2 Hello-Auth Check   : Enabled
L2 Csnp-Auth Check    : Enabled
L2 Psnp-Auth Check    : Enabled
Multi-Topology        : Disabled
Auto-Configuration    : Disabled
Area Address          : None
BFD Status            : Disabled
================================================================================
```

output definitions

System Id	The system ID of the router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
Admin State	The state of the router (**Up** or **Down**).
Protocols Enabled	The protocol enabled on the router: IPv4 or IPv6
Last Enabled	The date and time when the router is enabled.
Level Capability	The level capability of the router **(L1, L2,** or **L1L2**).
Authentication Check	Indicates the status of the authentication (**true** or **false**).
Authentication Type	The type of authentication (**simple**, **md5, keychain, none**).
Graceful Restart	Indicates if graceful restart is **Enabled** or **Disabled**.
GR helper-mode	Indicates if the helper mode of graceful restart is **Enabled** or **Disabled**.
LSP Lifetime	The Lifetime of the LSP (in seconds).
LSP Wait	The Wait time of the LSP (in seconds).
Adjacency Check	The adjacency check configuration on the router
L1 Auth Type	The authentication type (**simple**, **md5, keychain, none**) for Level-1 adjacency.
L2 Auth Type	The authentication type (**simple**, **md5, keychain, none**) for Level-2 adjacency.
L1 Wide Metrics-only	Indicates whether wide metrics is **Enabled** or **Disabled** for Level-1 adjacency.
L2 Wide Metrics-only	Indicates whether wide metrics is **Enabled** or **Disabled** for Level-2 adjacency.
L1 LSDB Overload	Indicates whether LSDB Overload is **Enabled** or **Disabled** for Level-1 adjacency.
L2 LSDB Overload	Indicates whether LSDB Overload is **Enabled** or **Disabled** for Level-2 adjacency.
L1 LSPs	The number of LSPs for Level-1 adjacency.
L2 LSPs	The number of LSPs for Level-2 adjacency.
Last SPF	The date and duration of the last SPF calculation.
SPF Wait	The Wait time for the SPF calculation.
Hello-Auth Check	Indicates the status of global Hello authentication check (**Enabled** or **Disabled**).
Csnp-Auth Check	Indicates the status of global CSNP authentication check (**Enabled** or **Disabled**).

output definitions (continued)

Psnp-Auth Check	Indicates the status of global PSNP authentication check (**Enabled** or **Disabled**).
L1 Hello-Auth Check	Indicates the status of L1 Hello authentication check (**Enabled** or **Disabled**).
L1 Csnp-Auth Check	Indicates the status of L1 CSNP authentication check (**Enabled** or **Disabled**).
L1 Psnp-Auth Check	Indicates the status of L1 PSNP authentication check (**Enabled** or **Disabled**).
L2 Hello-Auth Check	Indicates the status of L2 Hello authentication check (**Enabled** or **Disabled**).
L2 Csnp-Auth Check	Indicates the status of L2 CSNP authentication check (**Enabled** or **Disabled**).
L2 Psnp-Auth Check	Indicates the status of L2 PSNP authentication check (**Enabled** or **Disabled**).
Auto-Configuration	Indicates the status of auto-configuration for ISIS. (**Enabled** or **Disabled**)
Area Address	The area address of the router.
BFD Status	Indicates the status of IS-IS registration with BFD. (**Enabled** or **Disabled**).

Release History

Release 7.3.3; command introduced.
Release 7.3.4; **Auto-Configuration** field added.
Release 8.4.1.R03; **BFD Status** field added.

Related Commands

show ip isis statistics	Displays statistics for the IS-IS configuration.

MIB Objects

vRtrIsisTable

- vRtrIsisLastEnabledTime
- vRtrIsisAuthKey
- vRtrIsisAuthType
- vRtrIsisLspLifetime
- vRtrIsisOverloadTimeout
- vRtrIsisLastSpfRun
- vRtrIsisGracefulRestart
- vRtrIsisOverloadOnBootv
- vRtrIsisOverloadOnBootimeout
- vRtrIsisSpfWait
- vRtrIsisSpfInitialWait
- vRtrIsisSpfSecondWait
- vRtrIsisLspMaxWait
- vRtrIsisLspInitialWait
- vRtrIsisLspSecondWait
- vRtrIsisCsnpAuthentication
- vRtrIsisHelloAuthentication
- vRtrIsisPsnpAuthentication
- vRtrIsisGRHelperMode
- vRtrIsisSpfWait
- vRtrIsisMTEnabled

vRtrIsisLevelTable

- vRtrIsisLevelAuthKey
- vRtrIsisLevelAuthType
- vRtrIsisLevelExtPreference
- vRtrIsisLevelPreference
- vRtrIsisLevelWideMetricsOnly
- vRtrIsisLevelCsnpAuthentication
- vRtrIsisLevelPsnpAuthentication
- vRtrIsisLevelHelloAuthentication
- vRtrIsisLevelWideMertic
- vRtrIsisLevelNumLSPs

show ip isis summary-address

Displays the IS-IS summary address database.

show ip isis summary-address [*ip_address* **[***/mask***]]**

Syntax Definitions

ip_address	The 32-bit IP address.
/mask	The netmask value. The valid range is 1–32.

Defaults

By default summary address information for all the IP addresses is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the *ip_address* parameter with this command to view the summary address information for a specific IP address.

Examples

```
-> show ip isis summary-address
================================================================================
ISIS Summary Address
=====================================================
Address                     Level
--------------------------------------------------------------------------------
1.0.0.0/8                   L1
2.1.0.0/24                  L1L2
3.1.2.3/32                  L2
--------------------------------------------------------------------------------

Summary Address : 3
```

output definitions

Address	The summary address for a range of IPv4 addresses.
Level	The capability level of the router.
Summary Address	The number of summarized addresses.

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis summary-address	Adds or deletes the summary address.

MIB Objects

```
vRtrIsissummaryTable
   vRtrIsisSummPefix
   vRtrIsisSummMask
   vRtrIsisSummLevel
```

show ip isis vlan

Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

show ip isis vlan [*vlan_id***] [detail]**

Syntax Definitions

vlan_id	The VLAN ID.
detail	Indicates that the output is displayed in a detailed manner.

Defaults

By default, the interface information for all the interfaces is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the *vlan_id* parameter with this command to view information for a specific VLAN.

Examples

```
-> show ip isis vlan
================================================================================
ISIS VLan
================================================================================
Interface   Address-family  Level  VlanID  Oper-state   Admin-state  L1/L2-Metric
--------------------------------------------------------------------------------
ospf       ipv4           L1L2   11      DOWN       UP          10/10
vlan11      ipv6            L1L2    11      DOWN        UP           10/10
--------------------------------------------------------------------------------
Vlans : 2
================================================================================
```

output definitions

Interface	The name of the IS-IS interface.
Address-family	The address family extension: IPv4 or IPv6
Level	The level capability of the interface.
VlanID	The VLAN ID of the interface.
Oper-state	The operational state of the interface (**up** or **down**).
Admin-state	The administrative state of the interface (**up** or **down**).
L1/L2 -Metric	The metric value of the router for the corresponding capability level.
Vlans	The total number of VLANs.

```
-> show ip isis vlan detail
================================================================================
ISIS Interface
================================================================================
--------------------------------------------------------------------------------
VlanId             : 10             Level Capability  : L1L2
Oper State         : Up             Admin State       : Up
Auth Type          : Keychain(3)    Address Families  : IPv4, IPv6
Circuit Id         : 1              RetransmitInt     : 5
Type               : Broadcast      LSP Pacing Int    : 100
Mesh Group         : Inactive       CSNP Int          : 10
BFD Status         : Disabled

Level              : 1              Adjacencies       : 0
Desg IS            : abr_nyc
Auth Type          : None           Metric            : 10
Hello Timer        : 9              Hello Mult        : 3
Priority           : 64             Passive           : No
Level              : 2              Adjacencies       : 0
Desg IS            : abr_nyc
Auth Type          : None            Metric           : 10
Hello Timer        : 9               Hello Mult       : 3
Priority           : 64              Passive          : No
--------------------------------------------------------------------------------
VlanId             : 20              Level Capability : L1L2
Oper State         : Up              Admin State      : Up
Auth Type          : None            Address Families : IPv4, IPv6
Circuit Id         : 8               RetransmitInt    : 5
Type               : Pt-to-Pt        LSP Pacing Int   : 100
Mesh Group         : Inactive        CSNP Int         : 10
BFD Status         : Disabled

Level              : Pt-to-Pt
Desg  IS           : abr_nyc
Auth Type          : None            Metric           : 10
Hello Timer        : 9               Hello Mult       : 3
Priority           : 64              Passive          : No
--------------------------------------------------------------------------------
vlans : 2
================================================================================
```

output definitions

VlanId	The VLAN ID.
Level Capability	The level capability of the interface.
Oper State	The operational state of the interface (**up** or **down**).
Admin State	The administrative state of the interface (**up** or **down**).
Auth Type	Indicates the authentication type (**simple**, **MD5, keychain, none**) of the interface.
Address Families	The address family extension: IPv4 or IPv6
Circuit Id	The circuit ID of the interface.
RetransmitInt	Specifies the minimal interval of time, in seconds, between retransmission of an LSP on the point-to-point interface.
Type	The type of interface: **Broadcast** or **Pt-to-Pt** (point to point).

output definitions (continued)

LSP Pacing Int	The LSP Pacing interval.
Mesh Group	The status of the mesh group (**Active** or **Inactive**).
BFD Status	The status of BFD on the IS-IS VLAN interface (**Enabled** or **Disabled**).
CSNP Int	The CSNP interval.
Level	Indicates the IS-IS level of the neighbor (**L1, L2**, or **L1L2**).
Adjacencies	The number of adjacencies formed.
Desg IS	The ID of the LAN Designated Intermediate System on this circuit at this level.
Auth Type	Indicates the authentication type (**simple**, **MD5, keychain, none**) for the specified level.
Metric	The metric value of this circuit for a specific level.
Hello Timer	Indicates the Hello timer value.
Hello Mult	Indicates the Hello multiplier value.
Priority	The priority value of the interface.
Passive	Indicates whether the interface is configured as a passive interface (**Yes** or **No**).
Vlans	The total number of VLANs.

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis vlan	Configures IPv4 or IPv6 IS-IS circuit on a particular VLAN.

MIB Objects

```
 isisCircTable
   isisCircLocalID
   isisCircAdminState
   isisCircType
   isisCircLevel
   isisCircPassiveCircui
   isisCircMeshGroup
isisCircLevelTable
   isisCircLevelISPriority
   isisCircLevelCircID
   isisCircLevelDesIS
   isisCircLevelHelloMultiplier
   isisCircLevelHelloTimer
   isisCircLevelCSNPInterval
vRtrIsisIfTable
   vRtrIsisIfAdminState
   vRtrIsisIfOperState
   vRtrIsisIfCsnpInterval
   vRtrIsisIfHelloAuthKey
   vRtrIsisIfHelloAuthType
   vRtrIsisIfLspPacingInterval
   vRtrIsisIfRetransmitInterval
   vRtrIsisIfHelloAuthKeyChainId
vRtrIsisIfLevelTable
   vRtrIsisIfLevelHelloAuthKey
   vRtrIsisIfLevelHelloAuthType
   vRtrIsisIfLevelPassive
   vRtrIsisIfLevelNumAdjacencies
   vRtrIsisIfLevelISPriority
   vRtrIsisIfLevelHelloTimer
   vRtrIsisLevelOperMetric
   vRtrIsisIfLevelAdminMetric
   vRtrIsisIfLevelHelloAuthKeyChainId
```

show ip isis summary-address6

Displays the IS-IS IPv6 summary address database.

show ip isis summary-address6 [*ip_address* **[/***mask***]]**

Syntax Definitions

ip_address	The 32-bit IP address.
/mask	The netmask value. The valid range is 1–32.

Defaults

By default, summary address information for all the IP addresses is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the *ip_address* parameter with this command to view the summary address information for a specific IP address.

Examples

```
-> show ip isis summary-address6
============================================================
ISISv6 Summary Address
============================================================
Address                                     Level
------------------------------------------------------------
1111:1::/64                                 L1
------------------------------------------------------------
Summary Address : 1
============================================================
```

output definitions

Address	The summary address for a range of IPv6 addresses.
Level	The capability level of the router.
Summary Address	The number of summarized addresses.

Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis summary-address6	Configures the IPv6 summary address.

MIB Objects

N/A

clear ip isis adjacency

Clears and resets the IS-IS adjacency database information.

clear ip isis adjacency [system-id *nbr_sys_id***]**

Syntax Definitions

nbr_sys_id	The system ID of the neighbor router.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the *nbr_sys_id* parameter is specified, only the entries specific to that system ID are removed from the database.

Examples

```
-> clear ip isis adjacency system-id 1122.3344.5566
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis adjacency	Displays information about IS-IS adjacent routers.

MIB Objects

```
isisISAdjTable
   isisISAdjIndex
   isisISAdjState
   isisISAdjNeighSNPAAddress
   isisISAdjNeighSysType
   isisISAdjNeighSysID
   isisISAdjUsage
   isisISAdjHoldTimer
   isisISAdjNeighPriority
   isisISAdjUpTime
vRtrIsisISAdjTable
   vRtrIsisISAdjExpiresIn
   vRtrIsisISAdjCircLevel
   vRtrIsisISAdjRestartSupport
   vRtrIsisISAdjRestartStatus
   vRtrIsisISAdjRestartSupressed
```

clear ip isis lsp-database

Clears and resets the IS-IS LSP database information.

clear ip isis lsp-database [system-id *sys_id***]**

Syntax Definitions

sys_id	The system ID of the router.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the *sys_id* parameter is specified, only the entries specific to that system ID are removed from the database.

Examples

```
-> clear ip isis lsp-database system-id 000a.1234.2345
```

Release History

Release 7.3.3; command was introduced..

Related Commands

show ip isis database	Displays IS-IS LSP database information of the adjacent routers.

MIB Objects

```
vRtrIsisLSPTable
   vRtrIsisLSPId
   vRtrIsisLSPSeq
   vRtrIsisLSPChecksum
   vRtrIsisLSPLifetimeRemain
   vRtrIsisLSPVersion
   vRtrIsisLSPPktType
   vRtrIsisLSPPktVersion
   vRtrIsisLSPMaxArea
   vRtrIsisLSPSysIdLen
   vRtrIsisLSPAttributes
   vRtrIsisLSPUsedLen
   vRtrIsisLSPAllocLen
   vRtrIsisLSPBuff
   vRtrIsisLSPZeroRLT
```

clear ip isis spf-log

Clears and resets the IS-IS SPF log information.

clear ip isis spf-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> clear ip isis spf-log
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis spf-log	Displays the IS-IS SPF log.

MIB Objects

```
vRtrIsisSpfLogTable
   vRtrIsisSpfRunTime
   vRtrIsisSpfL1Nodes
   VRtrIsisSpfL2Nodes
   vRtrIsisSpfEventCount
   vRtrIsisSpfLastTriggerLSPId
   vRtrIsisSpfTriggerReason
```

clear ip isis statistics

Clears and resets the IS-IS statistics information.

clear ip isis statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> clear ip isis statistics
```

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis statistics	Displays the IS-IS statistics information.

MIB Objects

```
vRtrIsisStatsTable
   vRtrIsisSpfRuns
   vRtrIsisLSPRegenerations
   vRtrIsisInitiatedPurges
   vRtrIsisLSPRecd
   vRtrIsisLSPDrop
   vRtrIsisLSPSent
   vRtrIsisLSPRetrans
   vRtrIsisIIHRecd
   vRtrIsisIIHDrop
   vRtrIsisIIHSent
   vRtrIsisIIHRetrans
   vRtrIsisCSNPRecd
   vRtrIsisCSNPDrop
   vRtrIsisCSNPSent
   vRtrIsisCSNPRetrans
   vRtrIsisPSNPRecd
   vRtrIsisPSNPDrop
   vRtrIsisPSNPSent
   vRtrIsisPSNPRetrans
   vRtrIsisUnknownRecd
   vRtrIsisUnknownDrop
   vRtrIsisUnknownSent
   vRtrIsisUnknownRetrans
   vRtrIsisCSPFRequests
   vRtrIsisCSPFDroppedRequests
   vRtrIsisCSPFPathsFound
   vRtrIsisCSPFPathsNotFound
```

ip isis multi-topology

Enables M-ISIS (multi-topology) capability support for IS-IS. If enabled, IPv6 SPF computation is performed separate from the IPv4 SPF computation.

ip isis multi-topology

no ip isis multi-topology

Syntax Definitions

N/A

Defaults

By default, multi-topology is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Changing the multi-topology mode with this command results in internal disabling and re-enabling of the IS-IS protocol with the new mode of operation. This will cause IS-IS adjacencies to be reset.

Examples

```
-> ip isis multi-topology
-> no ip isis multi-topology
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show ip isis status	Displays the IS-IS status.
show ip isis adjacency	Displays information about IS-IS adjacent routers.

MIB Objects

```
vRtrIsisEntry
   vRtrIsisMTEnabled
```

29 BGP Commands

This chapter describes the CLI commands used to configure the BGP (Border Gateway Protocol) and Multiprotocol extensions to BGP. BGP is a protocol for exchanging routing information between gateway hosts in a network of ASs (autonomous systems). BGP is the most common protocol used between gateway hosts on the Internet. The routing table exchanged contains a list of known routers, the addresses they can reach, and a preference metrics associated with the path to each router so that the best available route is chosen.

Multiprotocol Extensions to BGP-4 supports the exchange of IPv6 unicast prefixes, as well as the establishment of BGP peering sessions with BGP speakers identified by their IPv6 addresses.

The OmniSwitch implementation of BGP-4 and Multiprotocol Extensions to BGP-4 complies with the following RFCs: 4271, 2439, 3392, 2385, 1997, 4456, 3065, 4273, 4760, 2545.

Note. In the following document, the BGP terms “peer” and “neighbor” are used interchangeably to mean any BGP speaker known to the local router.

MIB information for BGP is as follows:

Filename: ALCATEL-IND1-VIRTUALROUTER-MIB.mib
Module: alcatelIND1VirtualRouterMIB

Filename: ALCATEL-IND1-BGP-MIB.mib
Module: alcatelIND1BGPMIB

Filename: BGP4-MIB.mib
Module: bgp

The following table summarizes the available commands:

Global BGP Commands	**ip load bgp** **ip bgp admin-state** **ip bgp autonomous-system** **ip bgp bestpath as-path ignore** **ip bgp cluster-id** **ip bgp default local-preference** **ip bgp fast-external-failover** **ip bgp always-compare-med** **ip bgp bestpath med missing-as-worst** **ip bgp client-to-client reflection** **ip bgp as-origin-interval** **ip bgp synchronization** **ip bgp confederation identifier** **ip bgp maximum-paths** **ip bgp log-neighbor-changes** **ip bgp dampening** **ip bgp dampening clear** **ip bgp asn-format** **ip bgp unicast** **show ip bgp** **show ip bgp statistics** **show ip bgp dampening** **show ip bgp dampening-stats** **show ip bgp path** **show ip bgp routes**
Aggregate Configuration	**ip bgp aggregate-address admin-state** **ip bgp aggregate-address as-set** **ip bgp aggregate-address community** **ip bgp aggregate-address local-preference** **ip bgp aggregate-address metric** **ip bgp aggregate-address summary-only** **show ip bgp aggregate-address**
Network (local route) Configurations	**ip bgp network** **ip bgp network admin-state** **ip bgp network community** **ip bgp network local-preference** **ip bgp network metric** **show ip bgp network**

Neighbor (Peer) Configuration	**ip bgp neighbor** **ip bgp neighbor ttl-security** **ip bgp neighbor activate-ipv4** **ip bgp neighbor activate-ipv6** **ip bgp neighbor ipv6-nexthop** **ip bgp neighbor admin-state** **ip bgp neighbor advertisement-interval** **ip bgp neighbor clear** **ip bgp neighbor route-reflector-client** **ip bgp neighbor default-originate** **ip bgp neighbor timers** **ip bgp neighbor conn-retry-interval** **ip bgp neighbor auto-restart** **ip bgp neighbor maximum-prefix** **ip bgp neighbor md5 key** **ip bgp neighbor ebgp-multihop** **ip bgp neighbor description** **ip bgp neighbor next-hop-self** **ip bgp neighbor passive** **ip bgp neighbor remote-as** **ip bgp neighbor remove-private-as** **ip bgp neighbor soft-reconfiguration** **ip bgp neighbor stats-clear** **ip bgp confederation neighbor** **ip bgp neighbor update-source** **ip bgp neighbor in-aspathlist** **ip bgp neighbor in-communitylist** **ip bgp neighbor in-prefixlist** **ip bgp neighbor in-prefix6list** **ip bgp neighbor out-aspathlist** **ip bgp neighbor out-communitylist** **ip bgp neighbor out-prefixlist** **ip bgp neighbor out-prefix6list** **ip bgp neighbor route-map** **ip bgp neighbor clear soft** **show ip bgp neighbors** **show ip bgp neighbors policy** **show ip bgp neighbors timer** **show ip bgp neighbors statistics**
BGP BFD Commands	**ip bgp bfd-state** **ip bgp bfd-state all-neighbors** **ip|ipv6 bgp neighbor bfd-state**

Policy Commands	**ip bgp policy aspath-list** **ip bgp policy aspath-list action** **ip bgp policy aspath-list priority** **ip bgp policy community-list** **ip bgp policy community-list action** **ip bgp policy community-list match-type** **ip bgp policy community-list priority** **ip bgp policy prefix-list** **ip bgp policy prefix-list action** **ip bgp policy prefix-list ge** **ip bgp policy prefix-list le** **ip bgp policy prefix6-list** **ip bgp policy route-map** **ip bgp policy route-map action** **ip bgp policy route-map aspath-list** **ip bgp policy route-map asprepend** **ip bgp policy route-map community** **ip bgp policy route-map community-list** **ip bgp policy route-map community-mode** **ip bgp policy route-map lpref** **ip bgp policy route-map lpref-mode** **ip bgp policy route-map match-community** **ip bgp policy route-map match-mask** **ip bgp policy route-map match-prefix** **ip bgp policy route-map match-prefix6** **ip bgp policy route-map match-regexp** **ip bgp policy route-map med** **ip bgp policy route-map med-mode** **ip bgp policy route-map origin** **ip bgp policy route-map prefix-list** **ip bgp policy route-map prefix6-list** **ip bgp policy route-map weight** **ip bgp policy route-map community-strip** **show ip bgp policy aspath-list** **show ip bgp policy community-list** **show ip bgp policy prefix-list** **show ip bgp policy prefix6-list** **show ip bgp policy route-map**
BGP Graceful Restart Commands	**ip bgp graceful-restart** **ip bgp graceful-restart restart-interval**
IPv6 Global BGP Commands	**ipv6 bgp unicast** **show ipv6 bgp path** **show ipv6 bgp routes**
IPv6 BGP Network Configuration Commands	**ipv6 bgp network** **ipv6 bgp network community** **ipv6 bgp network local-preference** **ipv6 bgp network metric** **ipv6 bgp network admin-state** **show ipv6 bgp network**

IPv6 BGP Neighbor (Peer) Configuration Commands	**ipv6 bgp neighbor** **ipv6 bgp neighbor ttl-security** **ipv6 bgp neighbor activate-ipv4** **ipv6 bgp neighbor activate-ipv6** **ipv6 bgp neighbor ipv6-nexthop** **ipv6 bgp neighbor admin-state** **ipv6 bgp neighbor clear** **ipv6 bgp neighbor auto-restart** **ipv6 bgp neighbor remote-as** **ipv6 bgp neighbor timers** **ipv6 bgp neighbor maximum-prefix** **ipv6 bgp neighbor next-hop-self** **ipv6 bgp neighbor conn-retry-interval** **ipv6 bgp neighbor default-originate** **ipv6 bgp neighbor update-source** **ipv6 bgp neighbor ipv4-nexthop** **ipv6 bgp neighbor advertisement-interval** **ipv6 bgp neighbor description** **ipv6 bgp neighbor ebgp-multihop** **ipv6 bgp neighbor update-source-address** **ipv6 bgp neighbor passive** **ipv6 bgp neighbor remove-private-as** **ipv6 bgp neighbor soft-reconfiguration** **ipv6 bgp neighbor stats-clear** **ip bgp confederation neighbor6** **ipv6 bgp neighbor in-aspathlist** **ipv6 bgp neighbor in-communitylist** **ipv6 bgp neighbor in-prefixlist** **ipv6 bgp neighbor in-prefix6list** **ipv6 bgp neighbor out-aspathlist** **ipv6 bgp neighbor out-communitylist** **ipv6 bgp neighbor out-prefixlist** **ipv6 bgp neighbor out-prefix6list** **ipv6 bgp neighbor route-map** **ipv6 bgp neighbor clear soft** **ipv6 bgp neighbor route-reflector-client** **ipv6 bgp neighbor md5 key** **show ipv6 bgp neighbors** **show ipv6 bgp neighbors statistics** **show ipv6 bgp neighbors policy** **show ipv6 bgp neighbors timers**

ip load bgp

Loads the BGP protocol software into running memory on the router. The image file containing BGP should already be resident in flash memory before issuing this command.

ip load bgp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command requires that the BGP software be resident in flash memory in the active directory.
- Enter this command in the router's configuration file (boot.cfg) to ensure BGP software is running after a reboot.
- The command does not administratively enable BGP on the router; BGP will be disabled after issuing this command. You must issue the **ip bgp admin-state** to start the BGP protocol.

Examples

```
-> ip load bgp
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp autonomous-system	Configures the Autonomous system number for this BGP router.
ip bgp admin-state	Administratively enables or disables BGP.

MIB Objects

```
alaVrConfigTable
   alaVrConfigBgpStatus
```

ip bgp admin-state

Administratively enables or disables BGP. The BGP protocol will not be active until you enable it using this command.

ip bgp admin-state {enable | disable}

Syntax Definitions

enable	Enables BGP.
disable	Disables BGP.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- You must first load the BGP software into running memory using the **ip load bgp** command before initiating this command.
- Many BGP commands require that the protocol be disabled (**ip bgp admin-state**) before issuing them.

Examples

```
-> ip bgp admin-state enable
-> ip bgp admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip load bgp	Loads the BGP software.

MIB Objects

```
alaBgpGlobal
   alaBgpProtoStatus
```

ip bgp autonomous-system

Configures the Autonomous System (AS) number for this router. This number identifies this BGP speaker (this router) instance to other BGP routers. The AS number for a BGP speaker determines whether it is an internal or an external peer in relation to other BGP speakers. BGP routers in the same AS are internal peers while BGP routers in different ASs are external peers. BGP routers in the same AS exchange different routing information with each other than they exchange with BGP routers in external ASs. BGP speakers append their AS number to routes passing through them; this sequence of AS numbers is known as a route's AS path.

ip bgp autonomous-system *value*

Syntax Definitions

value	The AS number in the asplain, asdot+, or asdot formats.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A router can belong to only one AS. Do not specify more than one AS value for each router.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.
- The 4-octet ASN is represented in one of three ways:
  - asplain (simple decimal notation)
  - asdot+ (two 16-bit values as low-order and high-order)
  - asdot (a mixture of asplain and asdot+).

Examples

```
-> ip bgp autonomous-system 64724

The following examples show how to configure the local BGP ASN as 65535 in the
three different formats:
-> ip bgp autonomous-system 65535        (asplain format)
-> ip bgp autonomous-system 0.65535      (asdot+ format)
-> ip bgp autonomous-system 65535        (asdot format)

The following examples show how to configure the local BGP ASN as 65538 in the
three different formats:
-> ip bgp autonomous-system 65538              (asplain format
-> ip bgp autonomous-system 1.2                (asdot+ format)
-> ip bgp autonomous-system 1.2                (asdot format)
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.3; support for 4-octet ASN was added.

Related Commands

ip bgp admin-state	Enables and disables the BGP protocol.
ip bgp neighbor remote-as	Assigns an AS number to this BGP peer.

MIB Objects

```
alaBgpGlobal
   alaBgpAutonomousSystemNumber
```

ip bgp bestpath as-path ignore

Indicates whether AS path comparison will be used in route selection. The AS path is the sequence of ASs through which a route has traveled. A shorter AS path is preferred over a longer AS path. The AS path is always advertised in BGP route updates. This command informs BGP to use the length of the AS path as a criteria for determining the best route.

ip bgp bestpath as-path ignore

no ip bgp bestpath as-path ignore

Syntax Definitions

N/A

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this feature after it has been enabled.
- AS path comparison does not consider the type of links connecting the ASs along the path. In some cases a longer path over very fast connections may be a better route than a shorter path over slower connections. For this reason the AS path should not be the only criteria used for route selection. BGP considers local preference before AS path when making path selections.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp bestpath as-path ignore
-> no ip bgp bestpath as-path ignore
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address as-set	Specifies whether AS path aggregation is to be performed or not.
ip bgp policy aspath-list	Creates or removes an AS path list.
ip bgp default local-preference	Configures the default local preference (lpref) value to be used when advertising routes.

MIB Objects

```
alaBgpGlobal
   alaBgpAsPathCompare
```

ip bgp cluster-id

Configures a BGP cluster ID when there are multiple, redundant, route reflectors in a cluster. This command is not necessary for configurations containing only one route reflector.

ip bgp cluster-id *ip_address*

Syntax Definitions

ip_address	32-bit IP address that is the Cluster ID of the router acting as a route reflector.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- In a route-reflection configuration where there are multiple route-reflectors in a cluster, use this command to configure this cluster ID. Configuring multiple route-reflectors enhances redundancy and avoids a single point of failure. When there is only one reflector in a cluster, the router ID of the reflector is used as the cluster-ID.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.
- Using many redundant reflectors in a single cluster places demands on the memory required to store routes for all redundant reflectors' peers.

Examples

```
-> ip bgp cluster-id 1.2.3.4
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp admin-state	Enables and disables BGP.
ip bgp client-to-client reflection	Enables route reflection and sets this speaker as the route reflector.

MIB Objects

```
alaBgpGlobal
   alaBgpClusterId
```

ip bgp default local-preference

Configures the default local preference (lpref) value to be used when advertising routes. A higher local preference value is preferred over a lower value. The local preference value is sent to all BGP peers in the local autonomous system; it is not advertised to external peers.

ip bgp default local-preference *value*

Syntax Definitions

value	The default local preference value for this router. The valid range is 0–4294967295.

Defaults

parameter	default
value	100

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- Unless a route is specifically configured for a different local preference value it will default to value you specify in this command. This value is used for routes learned from external autonomous systems (the local preference value is not advertised in routes received from external peers) and for aggregates and networks that do not already contain local preference values.
- This value is specific to the router so it can compare its own local preference to those received in advertised paths. If other routers belong to the same AS, then they should use the same default local preference value.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp default local-preference 200
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address local-preference	Sets the local preference for a BGP aggregate.
ip bgp network local-preference	Sets the local preference for a BGP network.

MIB Objects

```
alaBgpGlobal
   alaBgpDefaultLocalPref
```

ip bgp fast-external-failover

Enables fast external failover (FEFO). When enabled, FEFO resets a session when a link to a directly connected external peer is operationally down. The BGP speaker will fall back to Idle and then wait for a connection retry by the external peer that went down.

ip bgp fast-external-failover

no ip bgp fast-external-failover

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable Fast External Failover.
- When enabled, this command allows BGP to take immediate action when a directly connected interface, on which an external BGP session is established, goes down. Normally BGP relies on TCP to manage peer connections. Fast External failover improves upon TCP by resetting connections as soon as they go down.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp fast-external-failover
-> no ip bgp fast-external-failover
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts a BGP peer.
ip bgp neighbor auto-restart	Enables or disables BGP peer automatic restart.
ip bgp neighbor timers	Configures the time interval between KEEPALIVE messages sent by this peer and the tolerated hold time interval, in seconds, for messages to this peer from other peers.

MIB Objects

```
alaBgpFastExternalFailOver
```

ip bgp always-compare-med

Enables or disables Multi-Exit Discriminator (MED) comparison between peers in different autonomous systems. The MED value is considered when selecting the best path among alternatives; it indicates the weight for a particular exit point from the AS. A path with a lower MED value is preferred over a path with a higher MED value.

ip bgp always-compare-med

no ip bgp always-compare-med

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable MED comparison for external peers.
- By default, BGP only compares MEDs from the same autonomous system when selecting routes. Enabling this command forces BGP to also compare MEDs values received from external peers, or other autonomous systems.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp always-compare-med
-> no ip bgp always-compare-med
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp bestpath med missing-as-worst	Configures the MED parameter when it is missing in a BGP path.

MIB Objects

```
alaBgpGlobal
   alaBgpMedAlways
```

ip bgp bestpath med missing-as-worst

Configures the MED parameter when it is missing in a BGP path.

ip bgp bestpath med missing-as-worst

no ip bgp bestpath med missing-as-worst

Syntax Definitions

N/A

Defaults

By default this command is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable missing MEDs as worst.
- This command is used to specify how a missing MED in an external BGP path is to be treated for route selection purposes. The default behavior is to treat missing MEDs as zero (best). This command allows you to treat missing MEDs as worst (2^{32}-1) for compatibility reasons.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp bestpath med missing-as-worst
-> no ip bgp bestpath med missing-as-worst
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp always-compare-med	Forces BGP to consider MED values from external routes.

MIB Objects

```
alaBgpGlobal
   alaBgpMissingMed
```

ip bgp client-to-client reflection

Enables or disables this BGP speaker (router) to be a route reflector. Route reflectors advertise routing information to internal BGP peers, referred to as *clients*. BGP requires all internal routers to know all routes in an AS. This requirement demands a fully meshed (each router has a direct connection to all other routers in the AS) topology. Route reflection loosens the fully meshed restriction by assigning certain BGP routers as route reflectors, which take on the responsibility of advertising routing information to local BGP peers.

ip bgp client-to-client reflection

no ip bgp client-to-client reflection

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the speaker as a route reflector.
- In addition to defining this router as the route reflector, this command also enable route reflection for this cluster. After setting this command this reflector will begin using route reflection behavior when communicating to client and non-client peers.
- Once route reflectors are configured, you need to indicate the clients (those routers receiving routing updates from the reflectors) for each route reflector. Use the **ip bgp neighbor route-reflector-client** command to configure clients.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp client-to-client reflection
-> no ip bgp client-to-client reflection
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp admin-state	Administratively disables BGP in this router.
ip bgp neighbor route-reflector-client	Configures a BGP peer to be a client to the this route reflector.

MIB Objects

```
alaBgpGlobal
   alaBgpRouteReflection
```

ip bgp as-origin-interval

Specifies the frequency at which routes local to the autonomous system are advertised. These advertisements are also referred to as UPDATE messages. This interval applies to advertisements to internal peers.

ip bgp as-origin-interval *seconds*

no ip bgp as-origin-interval

Syntax Definitions

seconds	The update interval in seconds. The valid range is 1–65535.

Defaults

parameter	default
seconds	15

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to reset the feature to the default value.
- A lower value may increase the likelihood of route flapping as route status is updated more frequently.

Examples

```
-> ip bgp as-origin-interval 15
-> no ip bgp as-origin-interval
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor advertisement-interval	Set the route advertisement interval for external peers.

MIB Objects

```
alaBgpGlobal
   alaBgpAsOriginInterval
```

ip bgp synchronization

Enables or disables synchronization of BGP prefixes with AS-internal routing information. Enabling this command will force the BGP speaker to advertise prefixes only if the prefixes are reachable through AS-internal routing protocols (IGPs like RIP and OSPF).

ip bgp synchronization

no ip bgp synchronization

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable IGP synchronization.
- A BGP router is not supposed to advertise routes learned through internal BGP updates unless those routes are also known by the primary internal routing protocol (e.g, RIP or OSPF). However, requiring all routers in an AS to know all external routes places a heavy burden on routers focusing mainly on Intra-AS routing. Therefore, disabling synchronization avoids this extra burden on internal routers. As long as all BGP routers in an AS are fully meshed (each has a direct connection to all other BGP routers in the AS) then the problem of unknown external router should not be a problem and synchronization can be disabled.
- By default, synchronization is disabled and the BGP speaker can advertise a route without waiting for the IGP to learn it. When the autonomous system is providing transit service, BGP should not propagate IGP paths until the IGP prefixes themselves are known to be reachable through IGP. If BGP advertises such routes before the IGP routers have learned the path, they will drop the packets causing a blackhole.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp synchronization
-> no ip bgp synchronization
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpIgpSynchStatus
```

ip bgp confederation identifier

Sets a confederation identification value for the local BGP speaker (this router). A confederation is a grouping of sub-ASs into a single AS. To peers outside a confederation, the confederation appears to be a single AS. Within the confederation multiple ASs may exist and even exchange information with each other as using external BGP (EBGP).

ip bgp confederation identifier *value*

Syntax Definitions

value	The confederation identification value. The valid range is 0–65535.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- A value of 0 means this local speaker is not a member of any confederation.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.
- Use this command in conjunction with the **ip bgp confederation neighbor** command to specify those peers that are a members of the same confederation as the local BGP speaker.

Examples

```
-> ip bgp confederation identifier 3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp autonomous-system	Sets the AS number for this router.
ip bgp confederation neighbor	Specifies peers that are members of a confederation.

MIB Objects

```
alaBgpGlobal
   alaBgpConfedId
```

ip bgp maximum-paths

Enables or disables support for multiple equal paths. When multipath support is enabled and the path selection process determines that multiple paths are equal when the router-id is disregarded, then all equal paths are installed in the hardware forwarding table. When multipath support is disabled, only the best route entry is installed in the hardware forwarding table.

ip bgp maximum-paths

no ip bgp maximum-paths

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable support for multiple equal cost paths.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp maximum-paths
-> no ip bgp maximum-paths
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpMultiPath
```

ip bgp log-neighbor-changes

Enables or disables the logging of peer state changes. If enabled, this logging tracks changes in the state of BGP peers from ESTABLISHED to IDLE and from IDLE to ESTABLISHED. Viewing peer state logging requires that certain debug parameters be set.

ip bgp log-neighbor-changes

no ip bgp log-neighbor-changes

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp log-neighbor-changes
-> no ip bgp log-neighbor-changes
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp admin-state	Disables BGP within the router.

MIB Objects

```
alaBgpGlobal
   alaBgpPeerChanges
```

ip bgp dampening

Enables or disables BGP route dampening or the suppression of unstable routes. Route dampening helps to control the advertisement of routes that are going up and then down at an abnormally high rate. Routes that are changing states (available then unavailable) are said to be *flapping*.

ip bgp dampening [half-life *half_life* **reuse** *reuse* **suppress** *suppress* **max-suppress-time** *max_suppress_time***]**

no ip bgp dampening

Syntax Definitions

half_life	The half-life duration, in seconds. The valid range is 0–65535.
reuse	The number of route withdrawals set for the re-use value. The valid range is 1–9999.
suppress	The dampening cutoff value. The valid range is 1–9999.
max_suppress_time	The maximum number of seconds a route can be suppressed. The valid range is 0–65535.

Defaults

parameter	value
half_life	300
reuse	200
suppress	300
max_suppress_time	1800

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable dampening.
- BGP dampening is disabled by default. When enabled, route dampening suppresses routes that are unstable, or “flapping,” and disrupting the network.
- BGP dampening of IPv6 route flaps is currently not supported.
- This command enables dampening and can also be used to change the default times for the dampening variables.
- Use the dampening variables to set penalties, suppression limits, and reuse values for flapping routes.

- The half-life value configures the half-life duration for a reachable route. After the time interval specified in this command, the penalty value for the route will be reduced by half. This command sets the duration in seconds during which the accumulated stability value is reduced by half if the route is considered reachable, whether suppressed or not. A larger value may be desirable for routes that are known for their instability. A larger value will also result in a longer suppression time if the route exceeds the flapping rate.
- The reuse value configures the number of route withdrawals necessary to begin readvertising a previously suppressed route. If the penalty value for a suppressed route fall below this value, then it will be advertised again. This command sets the reuse value, expressed as a number of route withdrawals. When the stability value for a route reaches or falls below this value, a previously suppressed route will be advertised again. The instability metric for a route is decreased by becoming more stable and by passing half-life time intervals.
- The suppress value configures the cutoff value, or number of route withdrawals, at which a flapping route is suppressed and no longer advertised to BGP peers. This value is expressed as a number of route withdrawals. When the stability value for a route exceeds this cutoff value, the route advertisement is suppressed.
- The max-suppress-time value configures the maximum time (in seconds) a route can be suppressed. This time is also known as the maximum holdtime or the maximum instability value. Once this time is reached the route flap history for a route will be deleted and the route will be advertised again (assuming it is still reachable). This maximum holdtime as applied on an individual route basis. Each suppressed route will be held for the amount of time specified in this command unless the route is re-advertised by falling below the reuse value.
- Entering the command with no variables returns the variables back to their defaults.

Examples

```
-> ip bgp dampening
-> ip bgp dampening half-life 20 reuse 800 suppress 60 max-suppress-time 40
-> no ip bgp dampening
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp dampening clear	Clears the dampening history data for all routes on the router, resetting route flap counters and unsuppressing any routes that had been suppressed due to route flapping violations.
show ip bgp dampening	Displays the BGP route dampening settings.
show ip bgp dampening-stats	Displays BGP dampening statistics.

MIB Objects

```
alaBgpGlobal
   alaBgpDampening
   alaBgpDampMaxFlapHistory
   alaBgpDampHalfLifeReach
   alaBgpDampReuse
   alaBgpDampCutOff
```

ip bgp dampening clear

Clears the dampening history data for all routes on the router, resetting route flap counters and unsuppressing any routes that had been suppressed due to route flapping violations.

ip bgp dampening clear

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to clear all of the currently stored information on routes for dampening purposes. When this command is entered, all route information in regards to dampening is cleared.
- BGP dampening of IPv6 route flaps is currently not supported.

Examples

```
-> ip bgp dampening clear
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp dampening	Enables or disables route dampening.

MIB Objects

```
alaBgpGlobal
   alaBgpDampeningClear
```

ip bgp asn-format

Configures the display format to be used when displaying 4-octet ASNs.

ip bgp asn-format {asdot | asplain}

Syntax Definitions

asdot	A mixture of asplain and asdot+.
asplain	Simple decimal notation.

Defaults

The default is **asplain**.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command configures the display format to be used when displaying 4-octet ASNs. This configuration changes only the output format. The input format can be in any mode.

Examples

```
-> ip bgp asn-format asdot
```

Release History

Release 7.3.3; command was introduced.

Related Commands

ip bgp autonomous-system	Configures the Autonomous System (AS) number for this router.
show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpAsnFormat
```

ip bgp aggregate-address

Creates and deletes a BGP aggregate route. Aggregate routes are used to reduce the size of routing tables by combining the attributes of several different routes and allowing a single aggregate route to be advertised to peers.

The base command (**ip bgp aggregate-address**) may be used with other keywords to set up aggregate address configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

Note that only one of the following optional keywords is specified with each use of the base command. Keywords are not combined together in a single command.

ip bgp aggregate-address *ip_address ip_mask*
[admin-state {enable | disable}]
[as-set]
[community *string***]**
[local-preference *value***]**
[metric *metric***]**
[summary-only]

no ip bgp aggregate-address *ip_address ip_mask*

Syntax Definitions

ip_address	32-bit IP address to be used as the aggregate address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete an aggregate route.
- This command allows administrative operations on a BGP aggregate. You must still enable the aggregate route through the **ip bgp aggregate-address admin-state** command.
- You cannot aggregate an address (for example, 100.10.0.0) if you do not have at least one more-specific route of the address (for example, 100.10.20.0) in the BGP routing table.
- Only the aggregate is advertised unless aggregate summarization is disabled using the **ip bgp aggregate-address summary-only** command.

Examples

```
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0
-> no ip bgp aggregate-address 172.22.2.0 255.255.255.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address summary-only	Enables or disables aggregate summarization, which suppresses more-specific routes.

MIB Objects

```
alaBgpAggrAddr
alaBgpAggrSet
alaBgpAggrCommunity
alaBgpAggrLocalPref
alaBgpAggrMetric
alaBgpAggrSummarize
alaBgpAggrMask
```

ip bgp aggregate-address admin-state

Enables or disables a BGP aggregate route.

ip bgp aggregate-address *ip_address ip_mask* **admin-state {enable | disable}**

Syntax Definitions

ip_address	32-bit IP address for this aggregate route.
ip_mask	32-bit subnet mask that determines how many bits of the network address denote the network number.
enable	Enables this aggregate route.
disable	Disables this aggregate route.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Configure all aggregate route parameters before enabling the aggregate with this command. Use the **ip bgp asn-format** command to configure individual aggregate parameters.
- The **show ip bgp path** command displays every aggregate currently defined.

Examples

```
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0 admin-state enable
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp asn-format	Creates an aggregate route.
show ip bgp path	Displays aggregate routes.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
```

ip bgp aggregate-address as-set

Specifies whether AS path aggregation is to be performed or not. AS path aggregation takes the AS path for all routes in this aggregate and creates a new AS path for the entire aggregate. This aggregated AS path includes all the ASs from the routes in the aggregate, but it does not repeat AS numbers if some routes in the aggregate include the same AS in their path.

ip bgp aggregate-address *ip_address ip_mask* **as-set**

no ip bgp aggregate-address *ip_address ip_mask* **as-set**

Syntax Definitions

ip_address	32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the **as-set** option.
- When AS path aggregation is disabled (the default), the AS path for the aggregate defaults to the AS number of the local BGP speaker (configured in the **ip bgp autonomous-system** command).
- If AS path aggregation is enabled, a flap in a more specific path's AS path will cause a flap in the aggregate as well.
- Do not use this command when aggregating many paths because of the numerous withdrawals and updates that must occur as path reachability information for the summarized routes changes.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 as-set
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 as-set
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp asn-format	Creates and deletes a BGP aggregate route.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrSet
```

ip bgp aggregate-address community

Defines a community for an aggregate route created by the **ip bgp aggregate-address** command. Communities are a way of grouping BGP peers that do not share an IP subnet or an AS number.

ip bgp aggregate-address *ip_address ip_mask* **community {none | no-export | no-advertise | no-export-subconfed |** *num:num***}**

Syntax Definitions

ip_address	32-bit IP address of the aggregate route.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon (AS:NN), as defined in RFC 1997.

Defaults

parameter	default
none | no-export | no-advertise | no-export-subconfed | *num:num*	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.
- To revert the aggregate community string to the default value, set the community string to **none**.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 community no-export
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 community none
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to **community** string.

Related Commands

ip bgp asn-format	Creates and deletes a BGP aggregate route.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrCommunity
```

ip bgp aggregate-address local-preference

Configures the local preference attribute value for this BGP aggregate. This value will override the default local preference value; it is used when announcing this aggregate to internal peers.

ip bgp aggregate-address *ip_address ip_mask* **local-preference** *value*

no ip bgp aggregate-address *ip_address ip_mask* **local-preference** *value*

Syntax Definitions

ip_address	An IP address for the aggregate route.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.
value	The local preference attribute. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to set the local preference back to the default value.
- You can specify that this route use the default local preference value for the AS by specifying zero (0). In this case the local preference for this route will take the default local preference value set for this AS (defined in the **ip bgp default local-preference** command).

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 local-preference 200
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 local-preference 200
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp default local-preference Sets the default local preference value for this AS.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrLocalPref
```

ip bgp aggregate-address metric

Configures the MED attribute value for a BGP aggregate. This value is used when announcing this aggregate to internal peers; it indicates the best exit point from the AS.

ip bgp aggregate-address *ip_address ip_mask* **metric** *value*

no ip bgp aggregate-address *ip_address ip_mask* **metric** *value*

Syntax Definitions

ip_address	A 32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.
value	The MED attribute. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to reset the aggregate metric back to its default value.
- The default value of zero indicates that a MED will not be sent for this aggregate. When a MED value is missing for a route, BGP will determine a MED value based upon the settings specified in the **ip bgp bestpath med missing-as-worst** command.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 metric 0
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 metric 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp bestpath med missing-as-worst	Configures the MED for paths that do not contain a MED value.
ip bgp always-compare-med	Forces BGP to use the MED for comparison of external routes.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrMetric
```

ip bgp aggregate-address summary-only

Enables or disables aggregate summarization, which supresses more-specific routes. Disabling aggregate summarization means that more-specific routes will be announced to BGP peers (internal and external peers).

ip bgp aggregate-address *ip_address ip_mask* **summary-only**

no ip bgp aggregate-address *ip_address ip_mask* **summary-only**

Syntax Definitions

ip_address	IP address for the aggregate route.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- This command specifies whether more-specific routes should be announced or suppressed.
- By default, aggregate summarization is enabled, which means that only the aggregate entry (for example, 100.10.0.0) is advertised. Advertisements of more-specific routes (for example, 100.10.20.0) are suppressed.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 summary-only
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 summary-only
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp asn-format	Creates and deletes a BGP aggregate route.

MIB Objects

```
alaBgpAggrTable
   alaBgpAggrAddr
   alaBgpAggrMask
   alaBgpAggrSummarize
```

ip bgp network

Creates or deletes a BGP network. A network must be known to the local BGP speaker; it also must originate from the local BGP speaker. The network may be directly connected, dynamically learned, or static.

In lieu of these options, the base command (**ip bgp network**) may be used with other keywords to set up network configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

ip bgp network *ip_address ip_mask*
[community *string***]**
[local-preference *value***]**
[metric *metric***]**
[admin-state {enable | disable}]

no ip bgp network *ip_address ip_mask*

Syntax Definitions

ip_address	32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a local network.
- Creating and enabling a network entry indicates to BGP that this network should originate from this router. The network specified must be known to the router, whether it is connected, static, or dynamically learned.
- You can create up to 200 network entries. The basic **show ip bgp path** command will display every network currently defined.
- This command allows administrative operations on a BGP network. You must still enable the network through the **ip bgp network admin-state** command.

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0
-> no ip bgp network 172.22.2.115 255.255.255.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network admin-state Enables a BGP network.

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetwrokMetric
   alaBgpNetworkLocalPref
   alaBgpNetworkCommunity
   alaBgpNetworkMask
```

ip bgp network admin-state

Enables or disables a BGP network.

ip bgp network *ip_address ip_mask* **admin-state {enable | disable}**

Syntax Definitions

ip_address	32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.
enable	Enables this network.
disable	Disables this network.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Configure all network parameters before enabling this BGP network with this command. Use the **ip bgp network** command to configure individual aggregate parameters.
- You can create up 200 network entries. The **show ip bgp path** command displays every network currently defined.

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network	Create a BGP network.
show ip bgp path	Display currently defined BGP networks.

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetworkMask
```

ip bgp network community

Defines a community for a route created by the **ip bgp network** command. Communities are a way of grouping BGP peers that do not share an IP subnet or an AS.

ip bgp network *ip_address ip_mask* **community {none | no-export | no-advertise | no-export-subconfed |** *num:num***}**

Syntax Definitions

ip_address	32-bit IP address of the network.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon (AS:NN), as defined in RFC 1997.

Defaults

parameter	default
none | no-export | no-advertise | no-export-subconfed | *num:num*	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.
- To revert the network community string to the default value, set the community string to **none**.

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 community export
-> ip bgp network 172.22.2.115 255.255.255.0 community none
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to **community** string.

Related Commands

ip bgp network	Creates or deletes a BGP network

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetworkMask
   alaBgpNetworkCommunity
```

ip bgp network local-preference

Defines the local preference value for a route generated by the **ip bgp network** command. This value will override the default local preference value; it is used when announcing this network to internal peers.

ip bgp network *ip_address ip_mask* **local-preference** *value*

no ip bgp network *ip_address ip_mask* **local-preference** *value*

Syntax Definitions

ip_address	32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.
value	The local preference attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to return the local preference of the specified network to its default setting.
- You can specify that this route use the default local preference value for the AS by specifying zero (0). In this case the local preference for this route will take the default local preference value set for this AS (defined in the **ip bgp default local-preference** command).

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 local-preference 600
-> no ip bgp network 172.22.2.115 255.255.255.0 local-preference 600
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network	Creates or deletes a BGP network.
ip bgp default local-preference	Sets the default local preference for this AS.

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetworkMask
   alaBgpNetworkLocalPref
```

ip bgp network metric

Configures the Multi-Exit Discriminator (MED) attribute value for an network generated by the **ip bgp network** command. This value is used when announcing this network to internal peers; it indicates the best exit point from the AS.

ip bgp network *ip_address ip_mask* **metric** *value*

no ip bgp network *ip_address ip_mask* **metric** *value*

Syntax Definitions

ip_address	32-bit IP address.
ip_mask	32-bit subnet mask that determines how many bits of the IP address denote the network number.
value	A MED attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to return the metric for this network to its default value.
- The default value of zero indicates that a MED will not be sent for this network. When a MED value is missing for a route, BGP will determine a MED value based upon the settings specified in the **ip bgp bestpath med missing-as-worst** command.

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 metric 100
-> no ip bgp network 172.22.2.115 255.255.255.0 metric 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network	Creates or deletes a BGP network.
ip bgp bestpath med missing-as-worst	Specifies the MED value when it is missing.

MIB Objects

```
alaBgpNetworkTable
   alaBgpNetworkAddr
   alaBgpNetworkMask
   alaBgpNetwrokMetric
```

ip bgp neighbor

Creates or deletes a BGP peer.

ip bgp neighbor *ip_address*

no ip bgp neighbor *ip_address*

Syntax Definitions

ip_address	32-bit IP address of the new BGP peer.

Defaults

No peers configured.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a BGP peer.
- You must still enable a BGP peer after creating it. A BGP peer is enabled using the **ip bgp neighbor admin-state** command.
- Once created, a BGP peer cannot be enabled until it is assigned an autonomous system number using the **ip bgp neighbor remote-as** command.

Examples

```
-> ip bgp neighbor 172.22.2.115
-> no ip bgp neighbor 172.22.2.115
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor admin-state	Enable or disable a BGP peer.
ip bgp neighbor remote-as	Configure the AS number for the peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
```

ip bgp neighbor ttl-security

Configures the Generalized TTL Security Mechanism (GTSM) for the BGP peer. GTSM allows to set the maximum number of hops for the IP packets between the switch and the peer. If the maximum number of hops exceeds, the packet is dropped at the NI.

ip bgp neighbor *ip_address* **ttl-security** *num*

ip bgp neighbor *ip_address* **no ttl-security**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
num	The maximum number of hops between the switch and the peer. The valid range for GTSM is 0 to 255.

Defaults

By default GTSM is disabled for communication with the peer.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- GTSM must be manually enabled on both peers in a connection.
- When GTSM is enabled, eBGP multihop must be disabled or vise-versa.
- Use the **no** form of this command to disable GTSM.

Examples

```
-> ip bgp neighbor 172.22.2.115 ttl-security 6
-> ip bgp neighbor 172.22.2.115 no ttl-security
```

Release History

Release 8.4.1; command was introduced.

Related Commands

show ip bgp neighbors	Displays the configured IPv4 BGP peers.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerTTLSecurityHops
```

ip bgp neighbor activate-ipv4

Enables the advertisement of IPv4 unicast capability to the IPv4 BGP peer.

ip bgp neighbor *ip_address* **[activate-ipv4]**

no ip bgp neighbor i*p_address* **[activate-ipv4]**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
activate-ipv4	Enable the advertisement of IPv4 unicast capability to the IPv4 BGP peer.

Defaults

By default, the command is enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to disable the advertisement of IPv4 unicast capability to IPv4 BGP peer.

Examples

```
-> ip bgp neighbor 172.22.2.115 activate-ipv4
-> no ip bgp neighbor 172.22.2.115 activate-ipv4
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerActivateIpv4
```

ip bgp neighbor admin-state

Enables or disables a BGP peer.

ip bgp neighbor *ip_address* **admin-state {enable | disable}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
enable	Enables this peer.
disable	Disables this peer.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- You must first create a peer and assign it an IP address using the **ip bgp neighbor** command before enabling the peer.
- Configure all BGP peer related commands before enabling a peer using this command. Once you enable the peer it will begin sending BGP connection and route advertisement messages.

Examples

```
-> ip bgp neighbor 172.22.2.115 admin-state enable
-> ip bgp neighbor 172.22.2.115 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Creates a BGP peer.
show ip bgp neighbors	Displays peer parameters.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
```

ip bgp neighbor advertisement-interval

Configures the time interval for updates between external BGP peers.

ip bgp neighbor *ip_address* **advertisement-interval** *value*

Syntax Definitions

ip_address	32-bit IP address of the neighbor.
value	An advertisement time interval in seconds. The valid range is 0–65535.

Defaults

parameter	default
value	30

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Internal peers sharing the same AS as the local BGP speaker (configured in the **ip bgp autonomous-system** command) use the global route advertisement update interval. This command sets the interval this peer uses to send BGP UPDATE messages to external peers.

Examples

```
-> ip bgp neighbor 172.22.2.115 255.255.255.0 advertisement-interval 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   bgpPeerMinRouteAdvertisementTinterval
```

ip bgp neighbor clear

Restarts a BGP peer. The peer will be unavailable during this restart.

ip bgp neighbor *ip_address* **clear**

Syntax Definitions

ip_address	32-bit IP address of the neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command whenever changes occur to BGP-related access lists, weights, distribution lists, timer specifications, or administrative distance.
- Many peer commands restart the peer as soon as they are configured. The following commands restart the BGP peer for which they are configured:
  - **ip bgp neighbor remote-as**
  - **ip bgp neighbor md5 key**
  - **ip bgp neighbor passive**
  - **ip bgp neighbor ebgp-multihop**
  - **ip bgp neighbor maximum-prefix**
  - **ip bgp neighbor update-source**
  - **ip bgp neighbor next-hop-self**
  - **ip bgp neighbor soft-reconfiguration**
  - **ip bgp neighbor route-reflector-client**
  - **ip bgp confederation neighbor**
  - **ip bgp neighbor remove-private-as**
  - **ip bgp neighbor update-source**.
- You do not need to issue the **ip bgp neighbor clear** command after issuing any of the above commands.

Examples

```
-> ip bgp neighbor 172.22.2.115 clear
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor auto-restart	Automatically attempts to restart a BGP peer session after a session terminates.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerRestart
```

ip bgp neighbor route-reflector-client

Configures this peer as a client to the local route reflector.

ip bgp neighbor *ip_address* **route-reflector-client**

no ip bgp neighbor *ip_address* **route-reflector-client**

Syntax Definitions

ip_address	32-bit IP address of the neighbor.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove this peer as a client to the local route reflector.
- This command configures this peer as one of the clients to the local route reflector.
- All of the peers configured using this command become part of the client group. The remaining peers are members of the non-client group for the local route reflector.
- When route reflection is configured all of the internal BGP speakers in an autonomous system need not be fully meshed. The route reflector take responsibility for passing internal BGP-learned routes to its peers.

Examples

```
-> ip bgp neighbor 172.22.2.115 route-reflector-client
-> no ip bgp neighbor 172.22.2.115 route-reflector-client
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp client-to-client reflection Configures the local BGP speaker as a route reflector

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerClientStatus
```

ip bgp neighbor default-originate

Enables or disables BGP peer default origination.

ip bgp neighbor *ip_address* **default-originate**

no ip bgp neighbor *ip_address* **default-originate**

Syntax Definitions

ip_address	32-bit IP address of the neighbor.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- When this command is enabled, the local BGP speaker advertises itself as a default to the peer. Such a default route overrides any learned default (propagation) and outbound policy. The default route 0.0.0.0 does not need to exist on the local router.

Examples

```
-> ip bgp neighbor 172.22.2.115 default-originate
-> no ip bgp neighbor 172.22.2.115 default-originate
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerDefaultOriginate
```

ip bgp neighbor timers

Configures the KEEPALIVE message interval and hold time interval (in seconds) with regards to the specified peer.

ip bgp neighbor *ip_address* **timers** *keepalive holdtime*

Syntax Definitions

ip_address	32-bit IP address for the BGP peer.
keepalive	The interval (in seconds) between KEEPALIVE messages. The valid values are zero (0) or the range 1–21845.
holdtime	The hold time interval between updates to peers, in seconds. The valid range is 0, 3–65535.

Defaults

parameter	default
keepalive	30
holdtime	90

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Configures the time interval between KEEPALIVE messages sent by this peer. KEEPALIVE messages do not contain route updates or indicate a change in the status of the BGP peer; they serve only to tell the receiving BGP peer that the connection is still live and the peer is reachable.
- By default, the keep alive interval of 30 seconds is one-third the default hold-time interval of 90 seconds. The keep alive interval can never be more than one-third the value of the hold-time interval. When the hold interval is reached without receiving keep alive or other updates messages, the peer is considered dead.
- Setting the keep alive value to zero means no keep alive messages will be sent.
- Once a connection is established with a peer and a time period of the length specified in this command transpires with no messages from the remote peer, then the connection with that remote peer will be considered dead.
- Configures the tolerated hold time interval, in seconds, for messages to this peer from other peers. The hold timer is used during the connection setup process and in on-going connection maintenance with BGP peers. If this peer does not receive a KEEPALIVE, UPDATE, or NOTIFICATION message within this time period, then the BGP connection will be closed.
- By default, the hold-interval of 180 seconds is three times the default keep-alive interval of 60 seconds. The hold-interval can never be less than three times the keep-alive value.

- You must restart the peer (using the **ip bgp neighbor clear** command) after issuing this command before the new hold time interval takes effect.
- Both values must be set at the same time.
- Entering this command without the variables resets the variables to their default value.

Examples

```
-> ip bgp neighbor 172.22.2.115 timers 80 240
-> ip bgp neighbor 172.22.2.115 timers
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor conn-retry-interval	The interval, in seconds, between BGP retries to set up a connection through the transport protocol with another peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   bgpPeerHoldTimeConfigured
   bgpPeerKeepAliveConfigured
```

ip bgp neighbor conn-retry-interval

The interval, in seconds, between BGP retries to set up a connection through the transport protocol with another peer. In the connect state, BGP tries to set up a connection with a remote peer. If the connection fails, then the connect retry interval is started. Once this interval elapses, BGP retries setting up the connection.

ip bgp neighbor *ip_address* **conn-retry-interval** *seconds*

Syntax Definitions

ip_address	32-bit IP address for the neighbor.
seconds	The time interval (in seconds) between retries. The valid range is 0–65535.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The time interval is started when a connection to a peer is lost.
- Other BGP peers may automatically attempt to restart a connection with this peer if they have configured automatic peer session restart (using the **ip bgp neighbor auto-restart** command).
- You must restart the peer (using the **ip bgp neighbor clear** command) after issuing this command before the new connection retry interval takes effect.
- Entering this command without the *seconds* variable resets the variable to its default value.

Examples

```
-> ip bgp neighbor 172.22.2.115 connect-interval 60
-> ip bgp neighbor 172.22.2.115 connect-interval
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor auto-restart	Enable automatic session restart after a session termination.
ip bgp neighbor clear	Restarts the peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   bgpPeerConnectRetryInterval
```

ip bgp neighbor auto-restart

Enables or disables BGP peer automatic restart. When enabled, this peer will automatically attempt to restart a session with another peer after a session with that peer terminates. When disabled, this peer will not try to re-establish a session with another peer after the session terminates; in such a case, the other peer will have to restart the session for the two peers to resume communication.

ip bgp neighbor *ip_address* **auto-restart**

Syntax Definitions

ip_address	32-bit IP address for the neighbor.

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable automatic peer restart.
- After a session with another peer terminates, the local BGP speaker will wait 60 seconds before attempting to restart the session. If the session does not start on the first attempt a second attempt will be made after another 120 seconds (60x2). On each unsuccessful session attempt, the previous delay between restarts is multiplied by 2, up to a maximum delay of 240 seconds. An exception to this rule occurs when the peer session terminates on receipt of a NOTIFY message with 'unsupported option' code or 'unsupported capability' code; in these cases the delay between restart attempts will begin at 1 second and multiply by 2 after each unsuccessful restart attempt (up to a maximum of 240 second delay).
- Disabling this option can be helpful in cases where other peers are prone to frequent flapping or sending many NOTIFY messages. By not restarting sessions with unstable neighbors, the local BGP speaker forces those unstable neighbors to re-initialize the connection.

Examples

```
-> ip bgp neighbor 172.22.2.115 auto-restart
-> no ip bgp neighbor 172.22.2.115 auto-restart
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Creates a BGP peer.
ip bgp neighbor admin-state	Enables a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerAutoRestart
```

ip bgp neighbor maximum-prefix

Configures the maximum number of prefixes, or paths, the local router can receive from this peer in UPDATE messages.

ip bgp neighbor *ip_address* **maximum-prefix** *maximum* **[warning-only]**

Syntax Definitions

ip_address	32-bit IP address for the BGP peer.
maximum	The maximum number of prefixes. The valid range is 0–4294967295.

Defaults

parameter	default
threshold	5000

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the number of prefixes sent by this peer reaches this limit, the peer is restarted.
- You can use BGP logging to receive a warning when the number of prefixes received from this peer reaches 80 percent of the value you configure in this command.
- If the **warning-only** prefix is used, the operator will be warned when the peer exceeds 80 percent of the configured number of maximum prefixes.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 maximum-prefix 1000
-> ip bgp neighbor 172.22.2.115 maximum-prefix 1000 warning only
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts the BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerMaxPrefixWarnOnly
   alaBgpPeerMaxPrefix
```

ip bgp neighbor md5 key

Sets an encrypted MD5 signature for TCP sessions with this peer in compliance with RFC 2385.

ip bgp neighbor *ip_address* **md5 key {***string* **| none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	The MD5 public key. Maximum character length is 200.
none	Removes the MD5 public key.

Defaults

parameter	default
string	no password

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Entering the keyword **none** in place of a key removes the password and disables authentication.
- Due to security concerns the actual password that you specify in this command is encrypted using a 3DES algorithm before it appears in a saved snapshot file. Also, if you were to view this command in a snapshot file, or **boot.cfg** file, it would appear in a different syntax. The syntax for this command used in snapshot files is as follows:

  ip bgp neighbor *ip_address* **md5 key-encrypt** *encrypted_string*

  However, you should not use this syntax to actually set an MD5 password; it will not work.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 md5 key openpeer5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts the BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerMD5Key
```

ip bgp neighbor ebgp-multihop

Allows external peers to communicate with each other even when they are not directly connected. The absence of communication between disconnected peers can occur when a router that is not running BGP sits between two BGP speakers; in such a scenario the BGP speakers are multiple hops from each other. By enabling this command, you allow the BGP peers to speak to each other despite the non-BGP router that sits between them.

ip bgp neighbor *ip_address* **ebgp-multihop [***ttl***]**

no ip bgp neighbor *ip_address* **ebgp-multihop**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
ttl	The Time to Live for the multi-hop connection, in seconds. The range is 1 to 255.

Defaults

parameter	default
ttl	255

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable multi-hop connections.
- By default an external BGP peer is on a directly connected subnet. This command allows you to configure an external BGP peer that is not directly connected and may be multiple hops away. It should be used with caution and only with the guidance of qualified technical support.
- As a safeguard against loops, the multi-hop connection will not be made if the only route to a multi-hop peer is the default route (0.0.0.0).
- The BGP peer is restarted after issuing this command.
- When eBGP multihop is enabled, GTSM must be disabled or vise-versa.

Examples

```
-> ip bgp neighbor 172.22.2.115 ebgp-multihop 250
-> no ip bgp neighbor 172.22.2.115 ebgp-multihop 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.
ip bgp neighbor next-hop-self	Sets the BGP peer to use next hop processing behavior.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerMultiHop
```

ip bgp neighbor description

Configures the BGP peer name.

ip bgp neighbor *ip_address* **description** *string*

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Peer name (1–20 characters).

Defaults

parameter	default
string	peer(ip_address)

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The peer name is a text identifier that, by default, follows the format “peer(x.x.x.x)” where x.x.x.x is the IP address of the BGP peer. For example, the default name of a peer at address 198.216.14.23 would be “peer(198.216.14.23)”.
- A peer name with embedded spaces must be enclosed in quotation marks.

Examples

```
-> ip bgp neighbor 172.22.2.115 description “peer for building 3”
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Sets the IP address for the peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerName
```

ip bgp neighbor next-hop-self

Sets the BGP peer to use next hop processing behavior. By default, the next-hop processing of BGP updates is disabled. Using this command to enable next-hop behavior may be useful in non-meshed networks where BGP peers do not have direct access to other peers.

ip bgp neighbor *ip_address* **next-hop-self**

no ip bgp neighbor *ip_address* **next-hop-self**

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable next hop processing behavior.
- In partially meshed networks a BGP peer may not have direct connections to other peers. When such a peer receives route updates from these distant peers (through other peers), it may treat the remote peer as if it were the next hop in the routing path. Packet forwarding will not work in such a case because no direct connection exists. This command allows this peer to deem itself the next hop on the routing path so that the two non-connected peers can route packets. This peer would have a direct connection to both peers that want to exchange packets.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 next-hop-self
-> no ip bgp neighbor 172.22.2.115 next-hop-self
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerNextHopSelf
```

ip bgp neighbor passive

Configures the local BGP speaker to wait for this peer to establish a connection. When enabled, the local BGP speaker will not initiate a peer session with this peer; in this sense, the BGP speaker is “passive.” When disabled, the local BGP speaker will attempt to set up a session with this peer.

ip bgp neighbor *ip_address* **passive**

no ip bgp neighbor *ip_address* **passive**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable passive peer behavior.
- By default BGP will initiate a session to a peer once the peer is configured, has an AS number, and is enabled. You can use this command to configure the local BGP speaker as passive and an outbound session will not be initiated to this peer. For such peers, BGP will always wait passively for the inbound session attempt.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 passive
-> no ip bgp neighbor 172.22.2.115 passive
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerPassive
```

ip bgp neighbor remote-as

Assigns an AS number to this BGP peer.

ip bgp neighbor *ip_address* **remote-as** *value*

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
value	Autonomous system number in the asplain, asdot+, or asdot formats.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A BGP peer created with the **ip bgp neighbor** command cannot be enabled (**ip bgp neighbor admin-state enable**) until it is assigned an autonomous system number. If the AS number matches the AS number assigned to the local BGP speaker (assigned using the **ip bgp autonomous-system** command), the peer is considered internal to the local autonomous system. Otherwise, the peer is consider external to the local BGP speaker's AS.
- This BGP peer may not be operational within this router and it may be in an external AS, but it must still be configured on this router before the local BGP speaker can establish a connection to the peer. The local BGP speaker does not auto-discover peers in other routers; it initially learns about peers through the peer commands.
- The BGP peer is restarted after issuing this command.
- The 4-octet ASN is represented in one of three ways:
  - asplain (simple decimal notation)
  - asdot+ (two 16-bit values as low-order and high-order)
  - asdot (a mixture of asplain and asdot+).

Examples

```
-> ip bgp neighbor 172.22.2.115 remote-as 100

The following examples show how to configure the BGP neighbor ASN as 65535 in the
three different formats:
-> ip bgp neighbor 2.2.2.2 remote-as 65535        (asplain format)
-> ip bgp neighbor 2.2.2.2 remote-as 0.65535      (asdot+ format)
-> ip bgp neighbor 2.2.2.2 remote-as 65535        (asdot format)
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.3; support for 4-octet ASN was added.

Related Commands

ip bgp autonomous-system	Set the AS for the local BGP speaker.
ip bgp neighbor	Create a BGP peer.
ip bgp neighbor admin-state enable	Enables a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerAS
```

ip bgp neighbor remove-private-as

Enables or disables the stripping of private autonomous system numbers from the AS path of routes destined to this peer.

ip bgp neighbor *ip_address* **remove-private-as**

no ip bgp neighbor *ip_address* **remove-private-as**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable stripping of private AS numbers.
- By default all AS numbers in the AS path are passed to peers. Enabling his command strips any private AS numbers in the AS path before sending updates to this peer. AS numbers in the range 64512 to 65535 are considered private ASs; they intended for internal use within an organization (such as an enterprise network), but they are not intended for use on public networks (such as the Internet).
- This command has no effect if you are not using ASs in the range 64512 to 65535.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 remove-private-as
-> no ip bgp neighbor 172.22.2.115 remove-private-as
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor remote-as	Configures the AS number for this peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerRemovePrivateAs
```

ip bgp neighbor soft-reconfiguration

Enables or disables BGP peer soft reconfiguration. Soft reconfiguration increases the stability of the peer by allowing you to reconfigure attributes that require peer resets without halting the TCP connection with other peers.

ip bgp neighbor *ip_address* **soft-reconfiguration**

no ip bgp neighbor *ip_address* **soft-reconfiguration**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Default

This command is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- This feature stores routes and other configuration information in local memory. When you make configuration changes that require a peer reset, the routing cache is not cleared and connections with other peers are not interrupted.
- If a peer is not route-refresh capable, by default, BGP stores all paths from peers, even those that are policy rejected, in anticipation of policy changes in the future. Storing these paths consumes memory. You can use this command to disable the storing of these paths, or soft reconfiguration. However, if soft reconfiguration is disabled and the peer is not route-refresh capable and the inbound policy changes, the peer will have to be restarted using the **ip bgp neighbor clear** command.
- If the peer is route-refresh capable and soft reconfiguration is disabled, inbound policy changes are still supported without re-starting the peer.

Examples

```
-> ip bgp neighbor 172.22.2.115 soft-reconfiguration
-> no ip bgp neighbor 172.22.2.115 soft-reconfiguration
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor clear	Restarts this BGP peer.
ip bgp neighbor clear soft	Invokes an inbound or outbound policy reconfiguration for a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerSoftReconfig
```

ip bgp neighbor stats-clear

Clears the statistics for a peer.

ip bgp neighbor *ip_address* **stats-clear**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command clears the statistical variables for a peer so they can accumulate from a known point.
- The cleared statistics include the total messages sent and received from this peer, the total UPDATE messages sent and received from this peer, the total NOTIFY messages sent and received from this peer, and the total peer state transition messages sent and received from this peer. These statistics can be displayed through **show ip bgp neighbors statistics**.

Examples

```
-> ip bgp neighbor 172.22.2.115 stats-clear
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp neighbors statistics	Displays peer statistics.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerClearCounter
```

ip bgp confederation neighbor

Configures this peer as a member of the same confederation as the local BGP speaker.

ip bgp confederation neighbor *ip_address*

no ip bgp confederation neighbor *ip_address*

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- You must first assign a confederation number to the local BGP speaker before assigning peers to the confederation. Use the **ip bgp confederation identifier** command to assign a confederation number to the local BGP speaker.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp confederation neighbor 172.22.2.115
-> no ip bgp confederation neighbor 172.22.2.115
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp confederation identifier	Sets a confederation identification value for the local BGP speaker (this router).

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerConfedStatus
```

ip bgp neighbor update-source

Configures the local address from which this peer will be contacted. This local address can be configured for internal and external BGP peers.

ip bgp neighbor *ip_address* **update-source [***interface_name***]**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
interface_name	The name of the interface.

Defaults

parameter	default
interface_address	0.0.0.0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This address does not override the router identification for this BGP peer (configured in the **ip bgp neighbor** command). It is the address through which this peer can be contacted within this router. The router identification for a peer, especially an external peer, may not exist in the local router, but that distant peer can still be contacted through this router. This command sets the local address through which this distant peer can be contacted.
- The default is restored by entering the command without a IP address.
- The BGP peer is restarted after issuing this command.
- The update-source is not related to the router-id, it specifies the interface to be used for the TCP connection endpoint. By default, the nearest interface is selected.

Examples

```
-> ip bgp neighbor 172.22.5.115 update-source 172.22.2.117
-> ip bgp neighbor 172.22.5.115 update-source vlan-22
-> ip bgp neighbor 172.22.5.115 update-source
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Sets the router identification for a BGP peer.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerLocalAddr
   alaBgpPeerLocalIntfName
```

ip bgp neighbor in-aspathlist

Assigns an inbound AS path list filter to a BGP peer.

ip bgp neighbor *ip_address* **in-aspathlist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Inbound AS path list (0 to 70 characters). This name is case sensitive.
none	Removes this AS path list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The AS path list name *(***InboundASpath** in the example below) is created using the **ip bgp policy aspath-list** command. Any inbound routes from the BGP peer must match this AS path filter before being accepted or passed to inbound policy.
- To deassign an input AS path filter list, use this command to assign a value of **none**.

Examples

```
-> ip bgp neighbor 172.22.2.115 in-aspathlist InboundASpath
-> ip bgp neighbor 172.22.2.115 in-aspathlist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy aspath-list	Creates or removes an AS path list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAspathListIn
```

ip bgp neighbor in-communitylist

Assigns an inbound community list filter to a BGP peer.

ip bgp neighbor *ip_address* **in-communitylist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Input community list (0 to 70 characters. This name is case sensitive.
none	Removes this community list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The community filter list name (**InboundCommlist** in the example below) is created using the **ip bgp policy community-list** command. Any inbound routes from the BGP peer must match this community filter before being accepted or passed to inbound policy.
- To deassign an input community filter list, use this command to assign a value of "**none**."

Examples

```
-> ip bgp neighbor 172.22.2.115 in-communitylist InboundCommlist
-> ip bgp neighbor 172.22.2.115 in-communitylist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerCommunityListIn
```

ip bgp neighbor in-prefixlist

Assigns an inbound prefix filter list to a BGP peer.

ip bgp neighbor *ip_address* **in-prefixlist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Input prefix filter list (0 to 70 characters). This name is case sensitive.
none	Removes this prefix list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix list name (**InboundPrefix** in the example below) is created using the **ip bgp policy prefix-list** command. Any inbound routes from the BGP peer must match this prefix filter before being accepted or passed to inbound policy.
- To deassign an input prefix filter list, use this command to assign a value of "**none.**"

Examples

```
-> ip bgp neighbor 172.22.2.115 in-prefixlist InboundPrefix
-> ip bgp neighbor 172.22.2.115 in-prefixlist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerPrefixListIn
```

ip bgp neighbor in-prefix6list

Assigns an inbound prefix6 list to a BGP peer.

ip bgp neighbor *ip_address* **in-prefix6list {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Input prefix6 filter list (0 to 70 characters). This name is case sensitive.
none	Removes this prefix6 list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix6 list name (**InboundPrefix6** in the example below) is created using the **ip bgp policy prefix6-list** command. Any inbound IPv6 routes from the BGP peer must match this prefix6 filter before being accepted or passed to inbound policy.
- To deassign an input prefix6 filter list, use this command to assign a value of "**none.**"

Examples

```
-> ip bgp neighbor 172.22.2.115 in-prefix6list InboundPrefix6
-> ip bgp neighbor 172.22.2.115 in-prefix6list none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerPrefix6ListIn
```

ip bgp neighbor out-aspathlist

Assigns an outbound AS path filter list to a BGP peer.

ip bgp neighbor *ip_address* **out-aspathlist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Outbound AS path list (0 - 70 characters).
none	Removes the AS path list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The AS path list name (**OutboundASpath** in the example below) is created using the **ip bgp policy aspath-list** command. Any outbound routes from the BGP peer must match this AS path filter, or policy, before being advertised or passed to outbound policy.
- To deassign an output AS path filter list, use this command to assign a value of "**none**".

Examples

```
-> ip bgp neighbor 172.22.2.115 out-aspathlist OutboundASpath
-> ip bgp neighbor 172.22.2.115 out-aspathlist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy aspath-list	Creates or removes an AS path list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAspathListOut
```

ip bgp neighbor out-communitylist

Assigns an outbound community filter list to a BGP peer.

ip bgp neighbor *ip_address* **out-communitylist {***string* **| none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Outbound community list (0 - 70 characters).
none	Removes the community list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The community filter list name (**OutboundCommlist** in the example below) is created using the **ip bgp policy community-list** command. Any outbound routes from the BGP peer must match this community filter before being advertised or passed to outbound policy.
- To deassign an output community filter list, use this command to assign a value of "**none**".

Examples

```
-> ip bgp neighbor 172.22.2.115 out-communitylist OutboundCommlist
-> ip bgp neighbor 172.22.2.115 out-communitylist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerCommunityListOut
```

ip bgp neighbor out-prefixlist

Assigns an outbound prefix filter list to a BGP peer.

ip bgp neighbor *ip_address* **out-prefixlist {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Output prefix filter list (0 - 70 characters).
none	Removes the prefix list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix list name (**OutboundPrefix** in the example below) is created using the **ip bgp policy prefix-list** command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to outbound policy.
- To deassign an output prefix filter list, use this command to assign a value of "**none**".

Examples

```
-> ip bgp neighbor 172.22.2.115 out-prefixlist OutboundPrefix
-> ip bgp neighbor 172.22.2.115 out-prefixlist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerPrefixListOut
```

ip bgp neighbor out-prefix6list

Assigns an outbound prefix6 filter list to a BGP peer.

ip bgp neighbor *ip_address* **out-prefix6list {***string* | **none}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
string	Output prefix6 filter list (0 - 70 characters).
none	Removes the prefix6 list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix6 list name (**OutboundPrefix6** in the example below) is created using the **ip bgp policy prefix6-list** command. Any outbound IPv6 routes from the BGP peer must match this prefix6 filter before being advertised or passed to outbound policy.
- To deassign an output prefix6 filter list, use this command to assign a value of "**none**".

Examples

```
-> ip bgp neighbor 172.22.2.115 out-prefix6list OutboundPrefix6
-> ip bgp neighbor 172.22.2.115 out-prefix6list none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerPrefix6ListOut
```

ip bgp neighbor route-map

Assigns a policy map (inbound or outbound) to a BGP peer.

ip bgp neighbor *ip_address* **route-map {***string* **| none} {in | out}**

no ip bgp neighbor *ip_address* **route-map {in | out}**

Syntax Definitions

ip_address	32-bit IP address of the peer.
string	Policy map name (0 to 70 characters). This name is case sensitive.
none	Deletes the route map if entered rather than a text string.
in	Designates this route map policy as an inbound policy.
out	Designates this route map policy as an outbound policy.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no f**orm of this command to deassign an inbound or an outbound policy.
- The policy route map name (**InboundRoute** in the example below) is created using the **ip bgp policy route-map** command. Any inbound routes from the BGP peer must match this route map filter before being accepted or passed to inbound policy.
- The policy route map name (**OutboundRoute** in the example below) is created using the **ip bgp policy route-map** command. Any outbound routes for the BGP peer must match this route map filter before being advertised or passed to outbound policy.
- It is also possible to deassign a route map by entering **none** in place of a route map name.

Examples

```
-> ip bgp neighbor 172.22.2.115 route-map InboundRoute in
-> ip bgp neighbor 172.22.2.115 route-map OutboundRoute out
-> ip bgp neighbor 172.22.2.115 route-map none in
-> no ip bgp neighbor 172.22.2.115 route-map in
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerRouteMapOut
   alaBgpPeerRouteMapIn
```

ip bgp neighbor clear soft

Invokes an inbound or outbound policy reconfiguration for a BGP peer.

ip bgp neighbor *ip_address* **clear soft {in | out}**

Syntax Definitions

ip_address	32-bit IP address of the BGP peer.
in	Applies reconfiguration to the inbound policies.
out	Applies reconfiguration to the outbound policies.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command reconfigures (or reapplies) all inbound or outbound policies to existing routes without restarting the peer session.
- This command is useful if policies have been changed.

Examples

```
-> ip bgp neighbor 172.22.2.115 clear soft in
-> ip bgp neighbor 172.22.2.115 clear soft out
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor soft-reconfiguration	Enables or disables BGP peer soft reconfiguration.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerReconfigureInBound
   alaBgpPeerReconfigureOutBound
```

ip bgp bfd-state

Enables or disables the registration of BGP with the BFD protocol.

ip bgp bfd-state {enable | disable}

Syntax Definitions

enable	Enables BFD for BGP.
disable	Disables BFD for BGP.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- BFD must be globally enabled for the switch and BGP must be registered with BFD at the protocol level before BGP can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and the BGP protocol acts based upon the BFD message.
- Whenever a neighbor goes down, BGP will inform BFD to remove that neighbor from the BFD active list.

Examples

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of BGP with the BFD protocol:

```
-> ip bgp bfd-state enable
-> ip bgp bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd admin-state	Enables or disables the global BFD protocol status for the switch.
ip bgp bfd-state all-neighbors	Enables or disables BFD for all BGP neighbors.
ip|ipv6 bgp neighbor bfd-state	Enables or disables BFD for a specific neighbor.
show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpBfdStatus
```

ip bgp bfd-state all-neighbors

Enables or disables BFD for all BGP neighbors.

ip bgp bfd-state all-neighbors {enable | disable}

Syntax Definitions

enable	Enables BFD for all the BGP neighbors.
disable	Disables BFD for all the BGP neighbors.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for BGP must be enabled before BGP can interact with BFD.

Examples

```
-> ip bgp bfd-state all-neighbors enable
-> ip bgp bfd-state all-neighbors disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp bfd-state	Enables or disables BGP with BFD protocol.
ip|ipv6 bgp neighbor bfd-state	Enables or disables the BFD for a specific BGP neighbor.
show ip bgp neighbors	Displays the configured IPv4 BGP peers.

MIB Objects

```
alaBgpGlobal
   alaBgpBfdAllNeighbors
```

ip|ipv6 bgp neighbor bfd-state

Enables or disables BFD for a specific IPv4 or IPv6 BGP neighbor.

{ip | ipv6} bgp neighbor {*ipv4_address* **|** *ipv6_address***} bfd-state {enable | disable}**

Syntax Definitions

ipv4_address	The IPv4 address of the BGP neighbor.
ipv6_address	The IPv6 address of the BGP neighbor.
enable	Enables BGP neighbor.
disable	Disables BGP neighbor.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for BGP must be enabled before BGP can interact with BFD.

Examples

```
-> ip bgp neighbor 135.10.10.2 bfd-state enable
-> ip bgp neighbor 135.10.10.2 bfd-state disable

-> ipv6 bgp neighbor fe80::2efa:a2ff:fe13:e402 bfd-state enable
-> ipv6 bgp neighbor fe80::2efa:a2ff:fe13:e402 bfd-state disable
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

Related Commands

ip bgp bfd-state	Enables or disables BGP with BFD protocol.
ip bgp bfd-state all-neighbors	Enables or disables BFD for all BGP neighbors.
show ip bgp neighbors	Displays the configured IPv4 BGP peers.

MIB Objects

```
alaBgpPeerEntry
   alaBgpPeerName
   alaBgpPeerBfdStatus
alaBgpGlobal
   alaBgpBfdAllNeighbors
```

ip bgp policy aspath-list

Creates or removes an AS path list.

ip bgp policy aspath-list *name* **"***regular_expression***"**

no ip bgp policy aspath-list *name* **"***regular_expression***"**

Syntax Definitions

name	AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	Regular expression, for example, "^100 200$" where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.

Defaults

No IP BGP peer policy AS path-list exists.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an AS path list.
- To create an AS path list, use the **ip bgp policy aspath-list** command.
- A regular expression consists of a character string presented in the form of a pattern, e.g., ^100 200$. Valid regular expression characters (metacharacters) are shown in the table below. See also "Configuring BGP" in your Advanced Routing Guide for more information on using regular expressions in BGP commands.

Symbol	Description
^	Matches the beginning of the AS path list.
123	Matches the AS number 123.
.	Matches any single AS number.
?	Matches zero or one occurrence of the previous token, which must be an AS number, a dot, an alternation or a range.
+	Matches one or more occurrences of the previous token, which must be an AS number, a dot, an alternation or a range.
*	Matches zero or more occurrences of the previous token, which must be an AS number, a dot, an alternation or a range.
(	Begins an alternation sequence of AS numbers. It matches any AS number listed in the alternation sequence.
|	Separates AS numbers in an alternation sequence.

Symbol	Description
)	Ends an alternation sequence of AS numbers
[	Begins a range pair consisting of two AS numbers separated by a dash. It matches any AS number within that inclusive range.
-	Separates the endpoints of a range.
]	Ends a range pair.
$	Matches the end of the AS path list.
,_	Commas, underscores and spaces are ignored.

- When using a regular expression in the CLI, the regular expression must be enclosed in quotation marks.
- This command creates AS path lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-aspathlist**, **ip bgp neighbor out-aspathlist**, **ipv6 bgp neighbor in-aspathlist**, and **ipv6 bgp neighbor out-aspathlist** commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies.
- If a BGP AS path list is configured to deny routes from a particular string of regular expression, then by default all of the routes coming from any AS would be denied. You must configure the policy instance in the same policy to allow other routes to come in, to be permitted from other ASs.
- General or more specific AS path list information can be displayed by varying the use of the **show ip bgp policy aspath-list** command.

Examples

```
-> ip bgp policy aspath-list InboundAspath "^100 200$"
-> ip bgp policy aspath-list OutboundAspath "^300 400$"
-> no ip bgp policy aspath-list InboundAspath "^100 200$"
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor out-aspathlist	Assigns an outbound AS path list filter to a BGP peer.
ip bgp policy aspath-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found.
ip bgp policy aspath-list priority	Configures priority for processing regular expressions in an AS path list.
ipv6 bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to an IPv6 BGP peer.
ipv6 bgp neighbor out-aspathlist	Assigns an outbound AS path filter list to an IPv6 BGP peer.

MIB Objects

```
alaBgpAspathMatchListTable
   alaBgpAspathMatchListRowStatus
```

ip bgp policy aspath-list action

Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found. Matching criteria are specified in the regular expression.

ip bgp policy aspath-list *name* **“***regular_expression***” action {permit | deny}**

Syntax Definitions

name	AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	Regular expression, e.g., “^100 200$” where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit | deny	permit

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A regular expression consists of a character string presented in the form of a pattern, e.g., ^100 200$. Refer to **ip bgp policy aspath-list** on page 29-108 for a table of valid regular expression characters (metacharacters). See also “Configuring BGP” in your Advanced Routing Guide for more information on using regular expressions in BGP commands.
- This command allows or stops AS path lists from being applied to a peer’s inbound and outbound routes configured through the **ip bgp neighbor in-aspathlist**, **ip bgp neighbor out-aspathlist**, **ipv6 bgp neighbor in-aspathlist,** and **ipv6 bgp neighbor out-aspathlist** commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies.
- General or more specific AS path list information can be displayed by varying the use of the **show ip bgp policy aspath-list** command.

Examples

```
-> ip bgp policy aspath-list InboundAspath “^100 200$” action permit
-> ip bgp policy aspath-list OutboundAspath “^300 400$” action deny
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor out-aspathlist	Assigns an outbound AS path list filter to a BGP peer.
ip bgp policy aspath-list	Creates or removes an AS path list.
ip bgp policy aspath-list priority	Configures priority for processing regular expressions in an AS path list.
ipv6 bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to an IPv6 BGP peer.
ipv6 bgp neighbor out-aspathlist	Assigns an outbound AS path filter list to an IPv6 BGP peer.

MIB Objects

```
alaBgpAspathMatchListTable
   alaBgpAspathMatchListAction
```

ip bgp policy aspath-list priority

Configures the priority for processing regular expressions in an AS path list.

ip bgp policy aspath-list *name* **"***regular_expression***" priority** *value*

Syntax Definitions

name	AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
regular_expression	Regular expression, e.g., "^100 200$" where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.
value	A priority value, e.g., 1, assigned to the policy action. Valid priority range is from 1 - 255.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A regular expression consists of a character string presented in the form of a pattern, e.g., ^100 200$. Refer to **ip bgp policy aspath-list** on page 29-108 for a table of valid regular expression characters (metacharacters). See also "Configuring BGP" in your Advanced Routing Guide for more information on using regular expressions in BGP commands.
- This command specifies the priority of an AS path list filter being applied to a peer's inbound and outbound routes configured through the **ip bgp neighbor in-aspathlist**, **ip bgp neighbor out-aspathlist**, **ipv6 bgp neighbor in-aspathlist**, and **ipv6 bgp neighbor out-aspathlist** commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies, but only in the order designated by the priority value.
- The higher the priority value specified in the command, the later the matching is processed. For example, regular expressions with a priority of 1 (the default) are processed before an expression assigned a priority of 3. When regular expressions have an equal priority, the processing order is indeterminate.
- General or more specific AS path list information can be displayed by varying the use of the **show ip bgp policy aspath-list** command.

Examples

```
-> ip bgp policy aspath-list InboundAspath "^100 200$" priority 1
-> ip bgp policy aspath-list OutboundAspath "^300 400$" priority 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor out-aspathlist	Assigns an outbound AS path list filter to a BGP peer.
ip bgp policy aspath-list	Creates or removes an AS path list.
ip bgp policy aspath-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found.
ipv6 bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to an IPv6 BGP peer.
ipv6 bgp neighbor out-aspathlist	Assigns an outbound AS path filter list to an IPv6 BGP peer.

MIB Objects

```
alaBgpAspathMatchListTable
   alaBgpAspathMatchListPriority
```

ip bgp policy community-list

Creates or deletes a community list.

ip bgp policy community-list *name* **{***num:num* | *num.num:num* | *num***}**

no ip bgp policy community-list *name* **{***num:num* | *num.num:num* | *num***}**

Syntax Definitions

name	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
num:num	The community number, given in the form of the AS number in the asplain format and the community number, separated by a colon.
num.num:num	The community number, given in the form of the AS number in the asdot or asdot+ format and the community number, separated by a colon.

Defaults

No IP BGP peer policy community-list exists.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a community-list.
- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.
- This command creates community lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-communitylist**, **ip bgp neighbor out-communitylist**, **ipv6 bgp neighbor in-communitylist** and **ipv6 bgp neighbor out-communitylist** commands. The community list filters routes based on one or more community match list strings, as shown in the example below. If the route matches the community list filter, according to the matching type *exact* or *occur*, then the *permit* or *deny* policy action associated with the match list string applies.
- General or more specific community list information can be displayed by varying the use of the **show ip bgp policy community-list** command.

Examples

```
-> ip bgp policy community-list CommListAIn 40:40
-> ip bgp policy community-list CommListAOut 400:20
-> no ip bgp policy community-list CommListAIn 40:40
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list match-type	Configures type of matching to be performed with a community string list.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.
ipv6 bgp neighbor in-communitylist	Assigns an inbound community list filter to an IPv6 BGP peer.
ipv6 bgp neighbor out-communitylist	Assigns an outbound community filter list to an IPv6 BGP peer.

MIB Objects

```
alaBgpCommunityMatchListTable
   alaBgpCommunityMatchListRowStatus
```

ip bgp policy community-list action

Configures the action to be taken for a community list when a match is found.

ip bgp policy community-list *name* **{none | no-export | no-advertise | no-export-subconfed |** *num:num***} action {permit | deny}**

Syntax Definitions

name	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon (AS:NN), as defined in RFC 1997.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit | deny	**permit**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- By default, this command allows routes that match the criteria specified in the community list to pass.
- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.

Examples

```
-> ip bgp policy community-list commListAIn 600:1 action permit
-> ip bgp policy community-list commListAIn 600:1 action deny
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to **community** string.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list match-type	Configures type of matching to be performed with a community string list.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.
ipv6 bgp neighbor in-communitylist	Assigns an inbound community list filter to an IPv6 BGP peer.
ipv6 bgp neighbor out-communitylist	Assigns an outbound community filter list to an IPv6 BGP peer.

MIB Objects

```
alaBgpCommunityMatchListTable
   alaBgpCommunityMatchListAction
```

ip bgp policy community-list match-type

Configures the type of matching to be performed with a community string list.

ip bgp policy community-list *name* **{none | no-export | no-advertise | no-export-subconfed |** *num:num***} match-type {exact | occur}**

Syntax Definitions

name	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
exact	Checks for an exact match of the community string and the community attribute.
occur	Checks for an occurrence of the community string anywhere in the community attribute.

Defaults

parameter	default
exact | **occur**	exact

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

By default, this command only allows routes to pass if the community string exactly matches the community attribute of the route.

Examples

```
-> ip bgp policy community-list commListC 600:1 match-type exact
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to **community** string.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.
ipv6 bgp neighbor in-communitylist	Assigns an inbound community list filter to an IPv6 BGP peer.
ipv6 bgp neighbor out-communitylist	Assigns an outbound community filter list to an IPv6 BGP peer.

MIB Objects

```
alaBgpCommunityMatchListTable
   alaBgpCommunityMatchListType
```

ip bgp policy community-list priority

Configures the priority for processing multiple items in a community list filter.

ip bgp policy community-list *name* **{none | no-export | no-advertise | no-export-subconfed |** *num:num***} priority** *value*

Syntax Definitions

name	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
value	Priority value in the range 0 - 255.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The higher the priority value specified in the command, the later the matching is processed. For example, items with a priority of 1 (the default) are processed before items assigned a priority of 3. When items have an equal priority, the processing order is indeterminate.

Examples

```
-> ip bgp policy community-list commListB 500:1 priority 3
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to **community** string.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list match-type	Configures type of matching to be performed with community string list.

MIB Objects

```
alaBgpCommunityMatchListTable
   alaBgpCommunityMatchListPriority
```

ip bgp policy prefix-list

Creates or deletes a prefix match list.

ip bgp policy prefix-list *name ip_address ip_mask*

no ip bgp policy prefix-list *name ip_address ip_mask*

Syntax Definitions

name	Prefix list name.
ip_address	IP address for the prefix list.
ip_mask	Mask for the prefix list.

Defaults

No IP BGP policy prefix-list exists.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command creates prefix lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-prefixlist**, **ip bgp neighbor out-prefixlist**, **ipv6 bgp neighbor in-prefixlist** and **ipv6 bgp neighbor out-prefixlist** commands. The prefix list filters routes based on one or more prefixes, as shown in the example below. If the route matches the prefix list filter, according to the **ge** (lower) and **le** (upper) limits defined, then the **permit** or **deny** action associated with the prefix applies.
- General or more specific prefix list information can be displayed by varying the use of the **show ip bgp policy prefix-list** command.

Examples

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-prefixlist	Assigns an inbound prefix filter list to a BGP peer.
ip bgp neighbor out-prefixlist	Assigns an outbound prefix filter list to a BGP peer.
ip bgp policy prefix-list action	Configures action to be taken for a prefix list when a match is found.
ip bgp policy prefix-list ge	Configures lower limit on length of prefix to be matched.
ip bgp policy prefix-list le	Configures upper limit on length of prefix to be matched.
ipv6 bgp neighbor in-prefixlist	Assigns an inbound prefix filter list to an IPv6 BGP peer.
ipv6 bgp neighbor out-prefixlist	Assigns an outbound prefix filter list to an IPv6 BGP peer.

MIB Objects

```
alaBgpPrefixMatchListTable
   alaBgpPrefixMatchListRowStatus
```

ip bgp policy prefix-list action

Configures the action to be taken for a prefix list when a match is found.

ip bgp policy prefix-list *name ip_address ip_mask* **action {permit | deny}**

Syntax Definitions

name	Prefix list name.
ip_address	IP address for the prefix list.
ip_mask	Mask for the prefix list.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit | deny	permit

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Configures the action to be taken for a prefix list when a match is found.

Examples

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0 action deny
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.
ip bgp policy prefix-list ge	Configures lower limit on length of prefix to be matched.
ip bgp policy prefix-list le	Configures upper limit on length of prefix to be matched.

MIB Objects

```
alaBgpPrefixMatchListTable
   alaBgpPrefixMatchListAction
```

ip bgp policy prefix-list ge

Configures the lower limit on the length of the prefix to be matched.

ip bgp policy prefix-list *name ip_address ip_mask* **ge** *value*

Syntax Definitions

name	Prefix list name.
ip_address	IP address for the prefix list.
ip_mask	Mask for the prefix list.
value	The lower limit value in the range 0 –32.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The default value of zero indicates there is no lower limit on the length of the prefix to be matched.
- This command is used in conjunction with the **ip bgp policy prefix-list le** command to set the prefix matching range. The two commands can be combined, as show in the Example section below.
- The **ge** (lower limit) value must be greater than or equal to the prefix length (8 in the example below) and less than or equal to the **le** (upper limit) value.

Examples

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.
ip bgp policy prefix-list action	Configures action to be taken for a prefix list when a match is found.
ip bgp policy prefix-list le	Configures upper limit on length of prefix to be matched.

MIB Objects

```
alaBgpPrefixMatchListTable
   alaBgpPrefixMatchListGE
```

ip bgp policy prefix-list le

Configures the upper limit on the length of the prefix to be matched.

ip bgp policy prefix-list *name ip_address ip_mask* **le** *value*

Syntax Definitions

name	Prefix list name.
ip_address	Prefix list IP address for the prefix list.
ip_mask	Prefix list mask for the prefix list.
value	The upper limit value in the range of 0 to 32.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The default value of zero indicates there is no upper limit on the length of the prefix to be matched. This command is used in conjunction with **ip bgp policy prefix-list ge** to set the prefix matching range. The two commands can be combined, as show in the Example section below.
- The **ge** (lower limit) value must be greater than or equal to the prefix length (8 in the example below) and less than or equal to the **le** (upper limit) value.

Examples

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.
ip bgp policy prefix-list action	Configures action to be taken for a prefix list when a match is found.
ip bgp policy prefix-list ge	Configures lower limit on length of prefix to be matched.

MIB Objects

```
alaBgpPrefixMatchListTable
   alaBgpPrefixMatchListLE
```

ip bgp policy prefix6-list

Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

ip bgp policy prefix6-list *pfx_list_name prefix6/pfx_length* **[action {permit | deny}] [admin-state {enable | disable}] [ge [**{*masklength*}**]] [le [**{*masklength*}**]]**

no ip bgp policy prefix6-list *pfx_list_name prefix6/pfx_length* **[action {permit | deny}] [admin-state {enable | disable}] [ge [**{*mask_length*}**]] [le [**{*mask_length*}**]]**

Syntax Definitions

pfx_list_name	Prefix list name.
prefix6	Prefix list IPv6 address for the prefix list.
pfx_length	Prefix length. Prefix length should be in the range of 0 to 128.
value	The upper limit value in the range of 0 to 32.
permit | **deny**	Action to be taken which can be either permit or deny.
enable | **disable**	Row Status can be either enabled or disabled.
mask_length	Minimum length of the prefix to be matched. The valid range is 0–32.

Defaults

NA

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- BGP must be configured on the system.
- This command creates prefix6 lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-prefix6list**, **ip bgp neighbor out-prefix6list**, **ipv6 bgp neighbor in-prefix6list** and **ipv6 bgp neighbor out-prefix6list**.
- The **ge** (lower limit) value must be greater than or equal to the prefix length and less than or equal to the **le** (upper limit) value.

Examples

```
-> ip bgp policy prefix6-list uniqLocal FC00::/48
-> ip bgp policy prefix6-list uniqLocal FC00::/48 action permit
-> ip bgp policy prefix6-list uniqLocal FC00::/48 admin-state enable
-> no ip bgp policy prefix6-list uniqLocal FC00::/48
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp policy prefix6-list	Displays prefix6 list parameters.
show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.
ip bgp neighbor in-prefix6list	Assigns an inbound prefix6 list to a BGP peer.
ip bgp neighbor out-prefix6list	Assigns an outbound prefix6 list to a BGP peer.
ipv6 bgp neighbor in-prefix6list	Assigns an inbound prefix6 list to an IPv6 BGP peer.
ipv6 bgp neighbor out-prefix6list	Assigns an outbound prefix6 list to an IPv6 BGP peer.

MIB Objects

```
alaBgpPrefix6MatchListTable
   alaBgpPrefix6MatchListId
   alaBgpPrefix6MatchListAddr
   alaBgpPrefix6MatchListAddrLength
   alaBgpPrefix6MatchListAction
   alaBgpPrefix6MatchListRowStatus
   alaBgpPrefix6MatchListGE
   alaBgpPrefix6MatchListLE
```

ip bgp policy route-map

Creates or deletes a policy route map.

ip bgp policy route-map *name sequence_number*

Syntax Definitions

name	Route map name. Case-sensitive.
sequence_number	Route map sequence number in the range of 1 to 255. The sequence number allows for multiple instances of the same route map name.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command creates policy route maps. Each route map can be configured using the following match commands to specify the match criteria by which routes are allowed to pass. Match criteria is examined in the order the commands are listed below.
  1. **ip bgp policy route-map aspath-list**
  2. **ip bgp policy route-map prefix-list**
  3. **ip bgp policy route-map prefix6-list**
  4. **ip bgp policy route-map community-list**
  5. **ip bgp policy route-map match-regexp**
  6. **ip bgp policy route-map match-prefix**
  7. **ip bgp policy route-map match-mask**
  8. **ip bgp policy route-map match-prefix6**
  9. **ip bgp policy route-map match-community**
- The route maps which apply to a specific address family (IPv4 or IPv6) are only applied to routes of the same address family. In other words, the prefix-list filter and match-prefix/match-mask route-maps are only applied to IPv4 routes and are ignored for IPv6 routes. The prefix6-list filter and match-prefix6 route-maps are only applied to IPv6 routes and are ignored for IPv4 routes.

- Each route map can also be configured using the following set commands to sequentially specify the actions to be taken when a match is found.
  - **ip bgp policy route-map community**
  - **ip bgp policy route-map community-mode**
  - **ip bgp policy route-map lpref**
  - **ip bgp policy route-map lpref-mode**
  - **ip bgp policy route-map med**
  - **ip bgp policy route-map med-mode**
  - **ip bgp policy route-map origin**
  - **ip bgp policy route-map weight**
- Route maps can be referenced as a filtering mechanism for displaying paths using the **show ip bgp path** command. They are also referenced in filtering inbound and outbound routes for BGP peers using the **ip bgp neighbor route-map** commands.

Examples

```
-> ip bgp policy route-map routemap1 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map action Configures action to be taken for a route when a match is found.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapRowStatus
```

ip bgp policy route-map action

Configures the action to be taken for a route when a match is found.

ip bgp policy route-map *name sequence_number* **action {permit | deny}**

Syntax Definitions

name	A route map name.
sequence_number	A route map sequence number. The valid range is 1–255.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing. In addition, no further instances (sequence numbers) of the route map are examined.

Defaultst

parameter	default
permit | deny	**permit**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

By default, this command allows routes that match the criteria specified in the route map to pass. If no matching routes are found, any additional instances (sequence numbers) of the route map name are examined. When all instances have been examined with no match, the route is dropped.

Examples

```
-> ip bgp policy route-map routemap1 1 action deny
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapAction
```

ip bgp policy route-map aspath-list

Assigns an AS path matching list to the route map.

ip bgp policy route-map *name sequence_number* **aspath-list** *as_name*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
as_name	The AS path list name or “none”.

Defaults

parameter	default
as_name	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- By default, no AS path list is assigned to a route map.
- This default behavior can be reset by changing the value of the AS path list name to “**none**”.
- The **ip bgp policy aspath-list** and **ip bgp policy aspath-list action** commands are used to create and set permit/deny actions for an AS path list.

Examples

```
-> ip bgp policy route-map routemap1 1 aspath-list aspathlist1
-> ip bgp policy route-map routemap1 1 aspath-list none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapAsPathMatchListId
```

ip bgp policy route-map asprepend

Configures the AS path prepend action to be taken when a match is found.

ip bgp policy route-map *name sequence_number* **asprepend** *path*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
path	The AS path to prepend or “none**”**. Note that multiple AS path entries must be enclosed in quotes (e.g., “500 600 700”).

Defaults

parameter	default
path	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

By default, no AS path is prepended. This command allows AS path numbers to be prepended (added to the beginning of the AS path list) to the AS path attribute of a matching route. The default behavior can be reset by changing the value to “none**”**.

Examples

```
-> ip bgp policy route-map routemap1 1 asprepend “700 800 900”
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapAsPrepend
```

ip bgp policy route-map community

Configures the action to be taken on the community attribute when a match is found.

ip bgp policy route-map *name sequence_number* **community [none | no-export | no-advertise | no-export-subconfed |** *num***:***num***]**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon (AS:NN), as defined in RFC 1997.

Defaults

parameter	default
none | no-export | no-advertise | no-export-subconfed | *num:num*	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- By default, no action is taken on a community attribute when a match on a route is found.
- The default behavior can be reset by setting the value to "**none**".
- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.
- The **ip bgp policy community-list** and **ip bgp policy community-list action** commands are used to create and set permit/deny actions for a community path list. This command is used in conjunction with **ip bgp policy route-map community-mode**.

Examples

```
-> ip bgp policy route-map routemap1 1 community 400:1 500:1
-> ip bgp policy route-map routemap1 1 community 400:1 500:1 community-mode replace
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map community-mode	Configures the action to be taken for a community string when a match is found.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapCommunity
```

ip bgp policy route-map community-list

Assigns a community matching list to the route map.

ip bgp policy route-map *name sequence_number* **community-list [***list_name* | **none]**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
list_name	The community list name.
none	No community list name is specified.

Defaults

parameter	default
list_name | **none**	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

By default, no community list is assigned to the route map. The default behavior can be reset by changing the value to **none**.

Examples

```
-> ip bgp policy route-map routemap1 1 community-list listB
-> ip bgp policy route-map routemap1 1 community-list none
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax **none** added to **community-list** string.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapCommunityMatchListId
```

ip bgp policy route-map community-mode

Configures the action to be taken for a community string when a match is found.

ip bgp policy route-map *name sequence_number* **community-mode {add | replace}**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
add	Adds the community string specified in the command **ip bgp policy route-map community**.
replace	Replaces the community string specified in the command **ip bgp policy route-map community**.

Defaults

parameter	default
add | replace	**add**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command is used in conjunction with **ip bgp policy route-map community**. The example on the next line shows the combined usage.

Examples

```
-> ip bgp policy route-map routemap1 1 community-mode replace
-> ip bgp policy route-map routemap1 1 community 400:1 500:1 community-mode replace
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map community	Configures the action to be taken on the community attribute when a match is found.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapSetComunityMode
```

ip bgp policy route-map lpref

Configures the local preference value for the route map.

ip bgp policy route-map *name sequence_number* **lpref** *value*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
value	The local preference value. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used in conjunction with **ip bgp policy route-map lpref-mode**. The example on the next line shows the combined usage.
- In this example, the local preference value will be incremented for a matching route by 555.

Examples

```
-> ip bgp policy route-map routemap1 1 lpref 555
-> ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map lpref-mode	Configures the action to be taken when setting local preference attribute for a local matching route.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapLocalPref
```

ip bgp policy route-map lpref-mode

Configures the action to be taken when setting local preference attribute for a local matching route.

ip bgp policy route-map *name sequence_number* **lpref-mode {none | inc | dec | rep}**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
none	Do not set the local preference attribute.
inc	Increment the local preference attribute in the matching route by the value specified in the **ip bgp policy route-map med** command. No action is taken if no local preference attribute is found in the matching route.
dec	Decrement the local preference attribute in the matching route by the value specified in the **ip bgp policy route-map med** command. No action is taken if no local preference attribute is found in the matching route.
rep	Replace the local preference attribute in the matching route by the value specified in the **ip bgp policy route-map med** command even if no local preference attribute is found in the matching route.

Defaults

parameter	default
none | inc | dec | rep	**none**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used in conjunction with **ip bgp policy route-map lpref**. The example below shows the combined usage.
- In this example, the local preference value is incremented for a matching route by 555.

Examples

```
-> ip bgp policy route-map routemap1 1 lpref-mode none
-> ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map lpref	Configures the local preference value for the route map.
ip bgp policy route-map med	Configures the Multi-Exit Discriminator (MED) value for a route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapLocalPrefMode
```

ip bgp policy route-map match-community

Configures a matching community primitive for the route map.

ip bgp policy route-map *name sequence_number* **match-community [none | no-export | no-advertise | no-export-subconfed |** *num:num***]**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
none	Removes the community match from the route-map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes matching the community restricting advertisement to any peer.
no-export-subconfed	Routes matching the community restricting advertisement to any external BGP peer.
num:num	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.

Defaults

parameter	default
none | **no-export** | **no-advertise** | **no-export-subconfed** | *num:num*	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows a matching community string primitive to be placed directly in the route map.
- By default, no community string is specified. The default behavior can be reset by changing the value to **none**.
- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.

Examples

```
-> ip bgp policy route-map routemap1 1 match-community 400:1 500 700:1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchCommunity
```

ip bgp policy route-map match-mask

Configures a matching mask primitive in the route map.

ip bgp policy route-map *name sequence_number* **match-mask** *ip_address*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
ip_address	The 32-bit IP address of the matching mask or “none”.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows a matching mask primitive to be placed directly in the route map. By default, no mask primitive is specified. The default behavior can be reset by changing the value to “**none**”.
- The example on the next line shows usage combined with the **ip bgp policy route-map match-prefix** command.

Examples

```
-> ip bgp policy route-map routemap1 1 match-mask 255.255.0.0
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0 match-mask 255.255.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.
ip bgp policy route-map match-prefix	Configures a matching prefix primitive in the route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchMask
```

ip bgp policy route-map match-prefix

Configures a matching prefix primitive in the route map.

ip bgp policy route-map *name sequence_number* **match-prefix** *ip_address*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
ip_address	The 32-bit IP address of the matching prefix.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows a matching prefix primitive to be placed directly in the route map. By default, no prefix primitive is specified. The default behavior can be reset by changing the value to "**none**".
- The example on the next line shows usage combined with the **ip bgp policy route-map match-mask** command.

Examples

```
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0 match-mask 255.255.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map match-mask	Configures a matching prefix primitive in the route map.
ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchPrefix
```

ip bgp policy route-map match-prefix6

Configures a matching prefix6 primitive in the route map.

ip bgp policy route-map *name sequence_number* **match-prefix6** *ipv6_address/mask_length*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
ipv6_address/mask_length	The 128-bit IPv6 address of the matching prefix. The length in bits of the IPv6 prefix to be matched in the Route Map.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command allows a matching prefix6 primitive to be placed directly in the route map. By default, no prefix6 primitive is assigned to the route map. The default behavior can be reset by changing the value to "**none**".

Examples

```
-> ip bgp policy route-map routemap1 1 match-prefix6 2001:1218:103::/64
-> ip bgp policy route-map routemap1 1 match-prefix6 none
```

Release History

Release 7.3.4; command introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchPrefix6
   alaBgpRouteMapMatchMaskLength6
```

ip bgp policy route-map match-regexp

Configures an AS path matching regular expression primitive in the route map.

ip bgp policy route-map *name sequence_number* **match-regexp "***regular_expression***"**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
regular_expression	Regular expression or "none". The regular expression must be enclosed by quotation marks.

Defaults

parameter	default
regular_expression	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command allows a regular expression matching directive to be placed directly in the route map. By default, no matching regular expression is specified. Regular expressions are defined in **ip bgp policy aspath-list** on page 29-108.
- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.
- The default behavior can be reset by changing the value to "**none**".
- See the *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide* for more information on the use of regular expressions in BGP commands.

Examples

```
-> ip bgp policy route-map routemap1 1 match-regexp "500 .* 400$"
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMatchAsRegExp
```

ip bgp policy route-map med

Configures the Multi-Exit Discriminator (MED) value for a route map.

ip bgp policy route-map *name sequence_number* **med** *value*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
value	The MED value. The valid range is 0–4294967295.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command is used in conjunction with **ip bgp policy route-map med-mode** command. The first example below shows the combined usage. In the second example, the MED value is incremented for a matching route by 5.

Examples

```
-> ip bgp policy route-map routemap1 1 med 555
-> ip bgp policy route-map routemap1 1 med 555 med-mode inc
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map med-mode	Configures Multi-Exit Discriminator (MED) value for a route map.
ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMed
```

ip bgp policy route-map med-mode

Configures the action to be taken when setting the Multi-Exit Discriminator (MED) attribute for a matching route.

ip bgp policy route-map *name sequence_number* **med-mode {none | inc | dec | rep}**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
value	The MED value. The valid range is 0–4294967295.
none	Do not set the MED.
inc	Increment the MED in the matching route by the value specified in the **ip bgp policy route-map med** command. No action is taken if no MED is found in the matching route.
dec	Decrement the MED in the matching route by the value specified in the **ip bgp policy route-map med** command. No action is taken if no MED is found in the matching route.
rep	Replace the MED in the matching route by the value specified in the **ip bgp policy route-map med** command even if no MED is found in the matching route.

Defaults

parameter	default
none | inc | dec | rep	**none**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command is used in conjunction with **ip bgp policy route-map med**. The first example below shows the combined usage. In the second example, the MED value is incremented for a matching route by 5.

Examples

```
-> ip bgp policy route-map routemap1 1 med-mode inc
-> ip bgp policy route-map routemap1 1 med 5 med-mode inc
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map med	Configures action to take when setting Multi-Exit Discriminator (MED) attribute for a matching route.
ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapMedMode
```

ip bgp policy route-map origin

Configures the action to be taken on the origin attribute when a match is found.

ip bgp policy route-map *name sequence_number* **origin {igp | egp| incomplete | none}**

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
igp	Sets the origin attribute to remote internal BGP (IGP).
egp	Sets the origin attribute to local external BGP (EGP).
incomplete	Sets the origin attribute to incomplete, meaning the origin is unknown.
none	Sets the origin attribute to “none”.

Defaults

parameter	default
igp | egp| incomplete | none	**none**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

By default, no action is taken on the origin attribute when a match is found. The default behavior can be reset by changing the value to “**none**”.

Examples

```
-> ip bgp policy route-map routemap1 1 origin egp
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map origin	Configures action to take on origin attribute when a match is found.
ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapOrgin
```

ip bgp policy route-map prefix-list

Assigns a prefix matching list to the route map.

ip bgp policy route-map *name sequence_number* **prefix-list** *prefix_name*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
prefix_name	The prefix list name or “none”.

Defaults

parameter	default
prefix_name	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- By default, no prefix list is assigned to the route map. The default behavior can be reset by changing the value to “**none**”.
- The **ip bgp policy prefix-list**, **ip bgp policy prefix-list action**, **ip bgp policy prefix-list ge**, and **ip bgp policy prefix-list le** commands are used to create and set permit/deny actions for a prefix path list.

Examples

```
-> ip bgp policy route-map routemap1 1 prefix-list listC
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Assigns a prefix matching list to the route map.
ip bgp policy prefix-list action	Configures action to be taken for a prefix list when a match is found.
ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapPrefixMatchListId
```

ip bgp policy route-map prefix6-list

Assigns a prefix6 matching list to the route map, which identifies the matching criteria list of IPv6 prefixes.

ip bgp policy route-map *name sequence_number* **prefix6-list** *prefix6_name*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
prefix_name	The prefix6 list name or “none”.

Defaults

parameter	default
prefix6_name	none

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix6-list policy name is created using the **ip bgp policy prefix6-list** command.
- By default, no prefix6 list is assigned to the route map. The default behavior can be reset by changing the value to “**none**”.

Examples

```
-> ip bgp policy route-map routemap1 1 prefix6-list listB
-> ip bgp policy route-map routemap1 1 prefix6-list none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapPrefix6MatchListId
```

ip bgp policy route-map weight

Configures a BGP weight value to be assigned to inbound routes when a match is found.

ip bgp policy route-map *name sequence_number* **weight** *value*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
value	The weight value. The valid range is 0–65535.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command sets the weight value for routes that pass the route map match criteria. It is only applicable for the inbound policy. The default value of zero means that the weight is not changed by the route map.

Examples

```
-> ip bgp policy route-map routemap1 1 weight 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapWeight
```

ip bgp policy route-map community-strip

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

ip bgp policy route-map *name sequence_number* **community-strip** *community_list*

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
community_list	The community list name.

Defaults

No IP BGP policy route-map community list exists.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

Examples

```
-> ip bgp policy route-map routemap1 1 commmunity_strip communitylist
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpRouteMapTable
   alaBgpRouteMapCommunityStrip
```

show ip bgp

Displays the current global settings for the local BGP speaker.

show ip bgp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Most of the parameters in this display can be altered through BGP global commands. See the output definitions below for references to the CLI commands used to configure individual parameters.

Examples

```
-> show ip bgp
Admin Status                         = disabled,
Operational Status                   = up,
Autonomous system Number             = 1,
BGP Router Id                        = 111.1.1.1,
Confederation Identifier             = 0,
IGP Synchronization Status           = disabled,
Minimum AS origin interval (seconds) = 15,
Default Local Preference             = 100,
Route Reflection                     = disabled,
Cluster Id                           = 0.0.0.0,
Missing MED Status                   = Best,
Aspath Comparison                    = enabled,
Always Compare MED                  = disabled,
Fast External Fail Over              = disabled,
Log Neighbor Changes                = disabled,
Multiple path                        = disabled,
Graceful Restart                     = enabled,
Graceful Restart Status              = Not Restarting,
Configured Graceful Restart Interval = 90s,
IPv4 Unicast                         = enabled,
IPv6 Unicast                         = disabled,
BFD Status                           = disabled,
ASN Output Format                    = asplain
```

output definitions

Admin Status	Indicates whether the BGP protocol has been enabled or disabled through the **ip bgp admin-state** command.
Operational Status	Indicates if the local BGP speaker is actively participating in BGP messages, update, routing advertisements.
Autonomous system Number	The AS assigned to the local BGP speaker through the **ip bgp autonomous-system** command.
BGP Router Id	The IP address for the local BGP speaker.
Confederation Id	Shows the confederation number assigned to the local BGP speaker. If the BGP speaker does not belong to a confederation, then this value will be zero (0). Confederation numbers are assigned through the **ip bgp confederation identifier** command.
IGP Synchronization Status	Indicates whether BGP is synchronizing its routing tables with those on non-BGP routers handling IGP traffic (such as a RIP or OSPF router). Configured through the **ip bgp synchronization** command.
Minimum AS origin interval	The frequency, in seconds, at which routes local to the autonomous system are advertised. Configured through the **ip bgp as-origin-interval** command.
Default Local Preference	The local preference that will be assigned to routes that do not already contain a local preference value. This default value is configured through the **ip bgp default local-preference** command.
Route Reflection	Indicates whether the local BGP speaker is acting as a route reflector for its AS. Configured through the **ip bgp client-to-client reflection** command.
Cluster Id	The IP address for cluster in route reflector configurations using multiple, redundant route reflectors. A value of 0.0.0.0 indicates that a cluster is not set up. Configured through the **ip bgp cluster-id** command.
Missing MED Status	Indicates the MED value that will be assigned to paths that do not contain MED values. Missing MED values will either be assigned to the worst possible value (2^{32}-1) or the best possible value (0). This value is set using the **ip bgp bestpath med missing-as-worst** command. By default, missing MED values are treated as **best**.
Aspath Comparison	Indicates whether the AS path will be in used in determining the best route. Configured through the **ip bgp bestpath as-path ignore** command.
Always Compare MED	Indicates whether multi-exit discriminator (MED) values are being compared only for internal peers or also for external peers. Configured through the **ip bgp always-compare-med** command.
Fast External Fail Over	Indicates whether Fast External Failover has been enabled or disabled. When enabled a BGP sessions will be reset immediately after a connection to a directly connected external peer goes down. Configured through the **ip bgp fast-external-failover** command.
Log Neighbor Changes	Indicates whether logging of peer state changes is enabled or disabled. Configured through the **ip bgp log-neighbor-changes** command.
Multi path	Indicates whether support for multiple equal cost paths is enabled or disabled. Configured through the **ip bgp maximum-paths** command.

output definitions (continued)

Graceful Restart	Indicates whether graceful restart is enabled or disabled.
Graceful Restart Status	Indicates the graceful restart state. This feature is not supported in Multiprotocol BGP.
Configured Graceful Restart Interval	Indicates the timer for achieving a graceful restart.
IPv4 Unicast	Indicates whether IPv4 unicast is enabled or disabled.
IPv6 Unicast	Indicates whether IPv6 unicast is enabled or disabled.
BFD Status	Indicates whether BFD is enabled or disabled for the BGP protocol. Configured through the **ip bgp bfd-state** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp unicast	Enables or disables unicast IPv4 updates for the BGP routing process.
ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process
show ip bgp statistics	Displays BGP global statistics.

MIB Objects

```
alabgpMIBGlobalsGroup
   alaBgpProtoStatus
   alaBgpAutonomousSystemNumber
   alaBgpIgpSynchStatus
   alaBgpProtoOperState
   alaBgpNumActiveRoutes
   alaBgpNumEstabExternalPeers
   alaBgpNumEstabInternalPeers
   alaBgpClusterId
   alaBgpDefaultLocalPref
   alaBgpFastExternalFailOver
   alaBgpMedAlways
   alaBgpMissingMed
   alaBgpRouterId
   alaBgpRouteReflection
   alaBgpAsOriginInterval
   alaNumIgpSyncWaitPaths
   alaBgpManualTag
   alaBgpPromiscuousneighbors
   alaBgpConfedId
   alaBgpMultiPath
   alaBgpMaxPeers
   alaBgpPeersChanges
```

show ip bgp statistics

Displays BGP global statistics.

show ip bgp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command show various BGP statistics for the router, such as number of neighbors, active prefixes, number of paths, etc.

Examples

```
-> show ip bgp statistics
# of Active Prefixes Known                = 0,
# of EBGP Neighbors in Established State  = 0,
# of IBGP Neighbors in Established State  = 0,
# of Feasible Paths                       = 0,
# of Dampened Paths                       = 0,
# of Unsynchronized Paths                 = 0,
# of Policy unfeasible paths              = 0,
Total Number of Paths                     = 0
```

output definitions

# of Active Prefixes Known	The number of prefixes, or route paths, currently known to the local BGP speaker, that are currently up and active.
# of EBGP Neighbors in Established State	The number of peers outside the AS of the local BGP speaker that the local BGP speaker can route to.
# of IBGP Neighbors in Established State	The number of peers in the same AS as the local BGP speaker that the local BGP speaker can route to.
# of Feasible Paths	The number of route paths that are not active due to one of the following reasons: the route is dampened, the route is not permitted based on BGP policies, or the route is waiting to be synchronized with the IGP protocol.
# of Dampened Paths	The number of route paths that are not active because they have violated dampening parameters.
# of Unsynchronized Paths	The number of route paths that are not active because they are waiting to be synchronized with the IGP routing protocol.

output definitions (continued)

# of Unfeasible Paths	The number of route paths that are not active because they are not permitted based on a configured BGP policy.
Total Number of Paths	The total number of paths known to the speaker, active or not.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpStatsTable
```

show ip bgp dampening

Displays the BGP route dampening settings.

show ip bgp dampening

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command shows the setting for dampening on the router, assuming it is enabled.

Examples

```
-> show ip bgp dampening
Admin Status                    = disabled,
Half life value (seconds)       = 300,
Reuse value                     = 200
Suppress value                  = 300,
Max suppress time (seconds)     = 1800,
```

output definitions

Admin Status	Indicates whether route dampening is enabled or disabled. This value is configured through the **ip bgp dampening** command.
Half life value	The half-life interval, in seconds, after which the penalty value for a reachable route will be reduced by half. This value is configured through the **ip bgp dampening** command.
Reuse value	The value that the route flapping metric must reach before this route is re-advertised. This value is configured through the **ip bgp dampening** command.
Suppress value	The number of route withdrawals necessary to begin readvertising a previously suppressed route. This value is configured through the **ip bgp dampening** command.
Max Suppress time	The maximum time (in seconds) that a route will be suppressed. This value is configured through the **ip bgp dampening** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp dampening	Enables or disables BGP route dampening or the suppression of unstable routes.

MIB Objects

```
alaBgpDampTable
   alaBgpDampEntry
   alaBgpDampCeil
   alaBgpDampCutOff
   alaBgpDampMaxFlapHistory
   alaBgpDampReuse
   alaBgpDampening
   alaBgpDampeningClear
```

show ip bgp dampening-stats

Displays BGP dampening statistics.

show ip bgp dampening-stats [*ip_address ip_mask*] [*peer_address*]

Syntax Definitions

ip_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.
peer_address	A 32-bit IP address of peer (neighbor).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays various statistics on routes that have flapped, and are thus subject to the settings of the dampening feature.

Examples

```
-> show ip bgp dampening-stats
Network         Mask            From            Flaps Duration    FOM
--------------+---------------+---------------+-----+-----------+-----
155.132.44.73   255.255.255.255 192.40.4.121    8     00h:00m:35s 175
```

output definitions

Network	The IP address for the local BGP speaker that is responsible for route dampening in this router.
Mask	The mask for the local BGP speaker that is responsible for route dampening in this router.
From	The IP address for the route that is flapping.
Flaps	The number of times this route has moved from an UP state to a DOWN state or from a DOWN state to an UP state. If the route goes down and then comes back up, then this statistics would count 2 flaps.
Duration	The time since the first route flap occurred. In the above example, this route has flapped 8 times in a 35 second period.
FOM	The Figure Of Merit, or instability metric, for this route. This value increases with each unreachable event. If it reaches the cutoff value (configured in **ip bgp dampening**), then this route will no longer be advertised.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp dampening	Enables and disables route dampening.

MIB Objects

N/A

show ip bgp path

Displays BGP paths.

show ip bgp path
[ip-addr *ip_address ip_mask***]**
[aspath-list *aspathlist_name***]**
[community-list *community_list_name***]**
[prefix-list *prefix_name***]**
[route-map *routemap_name***]**
[cidr-only]
[community *community_number***]**
[neighbor-rcv *recv_peer_address***]**
[neighbor-adv *adv_peer_addr***]**
[regexp "*regular_expression***"]**
[best]
[detail]

Syntax Definitions

ip_address	A 32-bit IP address of the path.
ip_mask	A 32-bit subnet mask of the path.
aspathlist_name	AS path on which to filter.
community_list_name	Community name on which to filter.
prefix_name	Prefix on which to filter.
routemap_name	Route map on which to filter.
cidr-only	Filter out everything except CIDR routes.
community_number	Community number on which to filter.
recv_peer_address	Filter all except paths received from this path.
adv_peer_addr	Filter all except paths sent to this path.
regular_expression	Regular expression on which to filter. Regular expressions must be enclosed by quotes. For example, "$100".
best	Show only the best path.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The basic command displays every path currently in the table. Since the number of paths may run into the thousands, this command provides a number of parameters for displaying a specific path or matching entries for a portion of a path or peer address.
- 'Detail' option displays the AS Path details for a specific route.

Examples

```
-> show ip bgp path
Legends: Sta     = Path state
         >       = best, F = feasible
         P       = policy changing, U = un-synchronized
         D       = dampened, N = none
         Nbr     = Neighbor
         (O)     = Path Origin (? = incomplete, i = igp, e = egp)
         degPref = degree of preference
Sta Network         Mask            Nbr address     Next Hop       (O)  degPref
---+--------------+---------------+--------------+--------------+---+--------
 >  192.40.4.0      255.255.255.0   192.40.4.29     192.40.4.29    i    100
 >  192.40.6.0      255.255.255.248 192.40.4.29     192.40.4.29    i    100
 >  192.40.6.8      255.255.255.248 192.40.4.29     192.40.4.29    i    100
 U  110.100.10.0    255.255.255.0   2001:100:3:4::1 110.100.10.20    ?    100
 U  110.100.11.0    255.255.255.0   2001:100:3:4::1 110.100.10.20    ?    100
 U  110.100.12.0    255.255.255.0   2001:100:3:4::1 110.100.10.20    ?    100
 U  110.100.13.0     255.255.255.0  2001:100:3:4::1 110.100.10.20    ?    100
 U  110.100.14.0     255.255.255.0  2001:100:3:4::1 110.100.10.20     ?    100

-> show ip bgp path detail
Legends: Sta     = Path state
         >       = best, F = feasible, S = stale
         P       = policy changing, U = un-synchronized
         D       = dampened, N = none
         Nbr     = Neighbor
         (O)     = Path Origin (? = incomplete, i = igp, e = egp)
         degPref = degree of preference
Sta  Network            Nbr address           Next Hop     degPref AS Path, (O)
---+-----------------+--------------------+-------------+-------+-----------
 >  192.168.1.0/32     20.20.20.2            20.20.20.2    100     65535 65530, i
 >  192.168.2.0/32     20.20.20.2            20.20.20.2    100     65535 65530, i
 >  192.168.3.0/32     20.20.20.2            20.20.20.2    100     65535 65530, i
 >  197.169.1.0/32      21.20.20.2           21.20.20.2    140     65536, i
 >  197.169.2.0/32      21.20.20.2           21.20.20.2    140     65536, i
 >  197.169.3.0/32      21.20.20.2           21.20.20.2    140     65536, i
```

output definitions

Sta	Status flag. A greater-than sign (>) indicates this is the best route to the destination.
Network	The IP address for this route path. This is the destination of the route.
Mask	The mask for this route path.
Nbr address	The IP or IPv6 address of the BGP peer that is advertising this path.
Next Hop	The next hop along the route path.

output definitions (continued)

(0)	The origin attribute of this route path. A question mark (**?**) indicates incomplete, and **i** indicates IGP, and an **e** indicates EGP.
degPref	The local preference value assigned to this route path.

```
-> show ip bgp path ip-addr 192.40.6.72 255.255.255.248
BGP Path parameters
Path address  = 192.40.6.72
Path mask     = 255.255.255.248
Path protocol = ebgp
Path peer     = 192.40.4.29
  Path nextHop            = 192.40.4.29,
  Path origin             = igp,
  Path local preference   = -1,
  Path state              = active,
  Path weight             = 0,
  Path preference degree  = 100,
  Path autonomous systems = [nAs=2] : 3 2 ,
  Path MED                = -1,
  Path atomic             = no,
  Path AS aggregator      = <none>,
  Path IPaddr aggregator  = <none>,
  Path community          = <none>,
  Path unknown attribute  = <none>
```

output definitions

Path address	The IP address for route path.
Path mask	The mask for this route path.
Path protocol	The protocol from which this route path was learned. Possible values for this field are as follows: **local**, **static**, **directhost**, **rip**, **ospf**, **isis**, **ibgp**, **ebgp**, and **other**.
Path peer	The IP address of the peer that is advertising this route path.
Path nextHop	The next hop along the route path.
Path origin	The BGP origin attribute. Possible values will be **igp**, **egp**, **incomplete**, and **none**. The origin attribute is considered during the route decision process.
Path local preference	The local preference value for this route as received in an UPDATE message. A negative value (for example, the **-1** in the above display) indicates that the local preference value is missing for this route path.
Path state	Path state indicates the state of the path.The possible states are **best**, **feasible**, **policy-wait**, **un-synchronized**, **dampened**, or **none**. When path state is **none**, it indicates that there are no paths to this prefix and the route is being purged from the system.
Path weight	The path weight as assigned through inbound and outbound policies.
Path preference degree	The local preference assigned to this route through an inbound or outbound policy, or, if the local preference value is missing, the default local preference (which is assigned through the **ip bgp default local-preference**).

output definitions (continued)

Path autonomous systems	The AS path for this route. These numbers show the ASs through which the route has traversed with the most recent AS listed first. In the above example, this route began its path in AS 2 and then traveled through AS 3.
Path MED	The multi-exit discriminator (MED) value for this route path. A negative value (for example, the **-1** in the above display) indicates that the MED value is missing for this route path.
Path atomic	Indicates whether the ATOMIC-AGGREGATE attribute has been set for this route. When set (this field would read **yes**), this attribute indicates that an aggregate has caused a loss of information for this route (a less specific route was chosen over a more specific route included in the aggregate).
Path AS aggregator	Part of the AGGREGATOR attribute. This field indicates the AS for the BGP speaker that created the aggregate. A value of **<none>** indicates this is not an aggregate route.
Path IPaddr aggregator	Part of the AGGREGATOR attribute. This field indicates the IP address for the BGP speaker that created the aggregate. A value of **<none>** indicates that this is not an aggregate route.
Path community	Indicates the community to which this route path belongs, if applicable. A value of **<none>** indicates that this route does not belong to a community.
Path unknown attribute	Indicates BGP attributes found in UPDATE messages which the router does not support. For example, multi-protocol attributes are not supported by the router in this release, but it is possible for these attributes to appear in a BGP route.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; ‘detail’ keyword added.

Related Commands

show ip bgp routes	Displays BGP route details.

MIB Objects

```
alaBgpPathTable
   alaBgpPathEntry
```

show ip bgp routes

Displays BGP route details.

show ip bgp routes [*ip_address ip_mask*]

Syntax Definitions

ip_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays all the routes in the routing table with details.

Examples

```
-> show ip bgp routes
Legends: ECL = EBGP change list, ICC = IBGP client change list
         ICL = IBGP change list, LCL = local change list
         AGG = Aggregation, AGC = Aggregation contribution
         AGL = Aggregation list, GDL = Deletion list
         AGW = Aggregation waiting, AGH = Aggregation hidden
         DMP = Dampening, ACT = Active route
Address         Mask            ECL ICC ICL LCL AGG AGC AGL AGW AGH GDL DMP ACT
--------------+---------------+---+---+---+---+---+---+---+---+---+---+---+---
192.40.4.0      255.255.255.0   No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.0      255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.8      255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.72     255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.80     255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.104    255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.112    255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
192.40.6.144    255.255.255.248 No  No  No  No  No  No  No  No  No  No  No  Yes
```

output definitions

Address	The route destination network address.
Mask	The route destination network mask.
ECL	External BGP change list. When Yes, this route will be advertised as soon as the route advertisement timer expires.
ICC	Internal BGP client change list. When Yes, this route will be advertised to internal non-clients.

output definitions (continued)

ICL	Internal BGP change list. When Yes, this route has changes that need to be advertised.
LCL	Local change list. When Yes, this route is local.
AGG	Aggregation. When Yes, this route is an aggregate route.
AGC	Aggregation contribution. When Yes, this route is part of an aggregate route.
AGL	Aggregation list. When Yes, this route is placed on an aggregate list.
AGW	Aggregation waiting. When Yes, this route is waiting for an aggregate contributor.
AGH	Aggregation hidden. When Yes, this route is hidden as part of an aggregate route.
GDL	Deletion list. When Yes, this route will be deleted.
DMP	Dampening. Indicate whether this route has been dampened. If 'Yes', then this route has been dampened and a dampening history exists.
ACT	Active route. When Yes, the route is active.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp path	Displays BGP paths.

MIB Objects

```
alaBgpRouteTable
   alaBgpRouteEntry
```

show ip bgp aggregate-address

Displays aggregate route status.

show ip bgp aggregate-address [*ip_address ip mask*]

Syntax Definitions

ip_address	A 32-bit IP address of the aggregate address.
ip_mask	A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays a specific aggregate address, or all aggregate addresses on the router.

Examples

```
-> show ip bgp aggregate-address
Network         Mask            Summarize As-Set   Admin state Oper state
--------------+---------------+---------+--------+-----------+----------
155.132.44.73   255.255.255.255 disabled  disabled disabled    not_active
192.40.6.0      255.255.255.255 disabled  disabled disabled    not_active

-> show ip bgp aggregate-address 192.40.6.0 255.255.255.255
Aggregate address          = 192.40.6.0,
Aggregate mask             = 255.255.255.255,
Aggregate admin state      = disabled,
Aggregate oper state       = not_active,
Aggregate as-set           = disabled,
Aggregate summarize        = disabled,
Aggregate metric           = 0,
Aggregate local preference = 0,
Aggregate community string = 0:500 400:1 300:2
```

output definitions

Network or **Aggregate address**	The IP address for this aggregate route. This value is configured through the **ip bgp aggregate-address** command.
Mask or **Aggregate mask**	The mask for this aggregate route. This value is configured through the **ip bgp aggregate-address** command.
Summarize or **Aggregate summarize**	Indicates whether aggregate summarization is enabled or disabled for this aggregate route. This value is configured through the **ip bgp aggregate-address summary-only** command.

output definitions (continued)

As-Set or **Aggregate as-set**	Indicates whether AS path aggregate is enabled or disabled. This value is configured through the **ip bgp aggregate-address as-set** command.
Admin State or **Aggregate admin state**	Indicates whether this aggregate route is administratively enabled or disabled. This value is configured through the **ip bgp aggregate-address admin-state** command.
Oper State or **Aggregate oper state**	Indicates whether this aggregate route is operational and participating in BGP message exchanges.
Aggregate metric	The multi-exit discriminator (MED) value configured for this aggregate route. This value is configured through the **ip bgp aggregate-address metric** command.
Aggregate local preference	The local preference value for this aggregate route. This value is configured through the **ip bgp aggregate-address local-preference** command.
Aggregate community string	The community string value for this aggregate route. This value is configured through the **ip bgp aggregate-address community** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address	Creates and deletes a BGP aggregate route.

MIB Objects

```
alabgpMIBAggrGroup
   alaBgpAggrSet
   alaBgpAggrLocalPref
   alaBgpAggrMetric
   alaBgpAggrSummarize
   alaBgpAggrCommunity
```

show ip bgp network

Displays currently defined network configurations.

show ip bgp network [*ip_address ip_mask*]

Syntax Definitions

ip_address	A 32-bit IP address.
ip_mask	A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays all the configured networks, or a single network.

Examples

```
-> show ip bgp network
Network         Mask            Admin state Oper state
--------------+---------------+-----------+----------
155.132.1.2     255.255.255.255 disabled    not_active
155.132.1.3     255.255.255.255 disabled    not_active

-> show ip bgp network 155.132.1.2 255.255.255.255
Network address          = 155.132.1.2,
Network mask             = 255.255.255.255,
Network admin state      = disabled,
Network oper state       = not_active,
Network metric           = 0,
Network local preference = 0,
Network community string = 0:500 400:1 300:2
```

output definitions

Network or **Network address**	The IP address configured for this local BGP network. This value is configured through the **ip bgp network** command.
Mask or **Network mask**	The mask configured for this local BGP network. This value is configured through the **ip bgp network** command.
Admin state or **Network admin state**	Indicates whether this local BGP network is administratively enabled or disabled. This value is configured through the **ip bgp network admin-state** command.

output definitions (continued)

Oper state or **Network oper state**	Indicates whether this BGP local network is operationally active or inactive.
Network metric	The multi-exit discriminator (MED) value configured for this local BGP network. This value is configured through the **ip bgp network metric** command.
Network local preference	The local preference value for this local BGP network. This value is configured through the **ip bgp network local-preference** command.
Network community string	The community string value for this local BGP network. This value is configured through the **ip bgp network community** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network	Configures a local BGP network.

MIB Objects

```
alabgpMIBNetworkGroup
   alaBgpNetworkEntry
```

show ip bgp neighbors

Displays the configured IPv4 BGP peers.

show ip bgp neighbors [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

There are two output options for this command. If you specify show ip bgp peer without a peer IP address, then you see summary information for all peers known to the local BGP speaker. If you enter a specific peer IP address with the command, then you see detailed parameter information for that peer only.

Examples

```
-> show ip bgp neighbors
Legends:Nbr = Neighbor
         As = Autonomous System
Nbr address   As        Admin state Oper state BGP Id       Up/Down      BFD Status
--------------+---------+-----------+----------+------------+------------+----------
192.40.4.29   3         enabled     estab      192.40.4.29  00h:14m:48s  disabled
192.40.4.121  5         disabled    idle       0.0.0.0      00h:00m:00s  enabled
```

output definitions

Nbr address	The IP address for this BGP peer. Assign this address through the **ip bgp neighbor** command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned through the **ip bgp neighbor remote-as** command.
Admin state	Indicates whether this peer has been enabled or disabled through the **ip bgp neighbor admin-state** command.
Oper state	The current BGP state for this peer. Possible states are **idle**, **connect**, **active**, **opensent**, **openconfirm**, and **established**.
BgpId	The unique BGP identifier of the peer. This value is configured through the **ip bgp neighbor update-source** command.

output definitions

Up/Down	The time since this peer has transitioned to its current UP or DOWN state. If the peer is currently Established, then this is the time that the peer has been UP. If the peer is currently Idle, then this is the time the peer has been DOWN.
BFD Status	Indicates whether BFD is enabled or disabled for this peer. The BFD status is configured through the **ip|ipv6 bgp neighbor bfd-state** command.

```
-> show ip bgp neighbors 0.0.0.1
Neighbor address                  = 0.0.0.1,
Neighbor autonomous system        = 1,
Neighbor Admin state              = enabled,
Neighbor Oper state               = connect,
Neighbor passive status           = disabled,
Neighbor name                     = peer(0.0.0.1),
Neighbor local address            = vlan-215,
Neighbor EBGP multiHop            = enabled,
Neighbor next hop self            = disabled,
Neighbor TTL security             = 6,
Neighbor Route Refresh            = enabled,
Neighbor Ipv4 unicast             = enabled,
Neighbor Ipv4 multicast           = disabled,
Neighbor type                     = internal,
Neighbor auto-restart             = enabled,
Neighbor route-reflector-client   = disabled,
Neighbor confederation status     = disabled,
Neighbor remove private AS        = disabled,
Neighbor default originate        = disabled,
Neighbor maximum prefixes         = 5000,
Neighbor max prefixes warning     = enabled,
# of prefixes received            = 0,
Neighbor MD5 key                  = <none>,
Neighbor local port               = 0,
Neighbor TCP window size          = 32768
Graceful Restart State            = None,
Advertised Restart Interval       = 0s,
Forwarding State during restart   = NotPreserved,
Activate IPv6 unicast             = enabled,
Configured IPv6 NextHop Address   = ::,
Neighbor Ipv6 unicast             = advertised
BFD Status                        = Disabled,
Activate IPv4 unicast             = enabled,
BFD Status                        = disabled,
Activate IPv4 unicast             = enabled
```

output definitions

Neighbor address	The IP address for this BGP peer. Assign this address through the **ip bgp neighbor** command.
Neighbor autonomous system	The autonomous system to which this peer belongs. A peer's AS number is assigned through the **ip bgp neighbor remote-as** command.
Neighbor Admin state	Indicates whether this peer has been enabled or disabled through the **ip bgp neighbor admin-state** command.

output definitions (continued)

Neighbor Oper state	The current BGP state for this peer. Possible states are **idle**, **connect**, **active**, **opensent**, **openconfirm**, and **established**.
Neighbor passive status	Indicates whether the local BGP speaker is "passive" (i.e., waiting for this peer to initiate a session). This value is configured through the **ip bgp neighbor passive** command.
Neighbor name	The name assigned to this peer through the **ip bgp neighbor description** command.
Neighbor local address	The interface assigned to this peer. This value is configured through the **ip bgp neighbor update-source** command.
Neighbor EBGP multihop	Indicates whether BGP multi-hop support is enabled or disabled. This supports allows external BGP peers to communicate with each other even when they are not directly connected. This value is configured through the **ip bgp neighbor ebgp-multihop** command.
Neighbor next hop self	Indicates whether this peer is using next hop processing. This value is configured through the **ip bgp neighbor next-hop-self** command.
Neighbor TTL security	Displays the number of hops between the switch and the peer. If the GTSM is disabled the value is displayed as none.
Neighbor Route Refresh	Indicates whether this peer supports Route Refresh capability as defined in RFC 2918. This capability is an alternative to soft-reconfiguration that can save CPU and memory resources. It allows peers to dynamically request the re-advertisement of BGP routing tables. Since this router supports route refresh all BGP peers are automatically enabled for this capability.
Neighbor Ipv4 unicast	Indicates whether this peer is multi-protocol IP version 4 unicast capable. This router is IPv4 unicasts capable so all peers will be enabled for this capability.
Neighbor Ipv4 multicast	Indicates whether this peer is multi-protocol IP version 4 multicast capable. This router is not IPv4 multicasts capable so all peers will be disabled for this capability.
Neighbor type	Indicates whether this peer is internal or external to the router.
Neighbor auto-restart	Indicates whether peer auto-restart is enabled or disabled. This value is configured through the **ip bgp neighbor auto-restart** command.
Neighbor route-reflector-client	Indicates whether this peer is a client to the local route reflector, if configured. This value is configured through the **ip bgp neighbor route-reflector-client** command.
Neighbor confederation status	Indicates whether this peer is a member of a BGP confederation. This value is configured through the **ip bgp confederation neighbor** command.
Neighbor remove private AS	Indicates whether the stripping of private AS numbers (64512 to 65535) from AS paths is enabled or disabled. This value is configured through the **ip bgp neighbor remove-private-as** command.
Neighbor default originate	Indicates whether peer default origination is enabled or disabled. When enabled, the local BGP speaker advertises itself as a default to the peer. This value is configured through the **ip bgp neighbor default-originate** command.

output definitions (continued)

Neighbor maximum prefixes	The maximum number of prefixes the local router can receive in UPDATE from this peer. This value is configured through the **ip bgp neighbor maximum-prefix** command.
Neighbor max prefixes warning	Indicates whether a warning will be issued when this peer exceeds 80 percent of the maximum prefix value. This value is configured through the **ip bgp neighbor update-source** command.
# of prefixes received	Displays the total number of prefixes received by this neighbor.
Neighbor MD5 key [32- 47]	When present, shows an encrypted version of the MD5 password. When not present, and MD5 password has not been configured. This value is configured through the **ip bgp neighbor md5 key** command.
Neighbor local port	The TCP port used for the session with this peer.
Neighbor TCP window size	The size of the TCP window for this BGP session. This value will always be 32768 as that is the maximum size of a BGP message.
Graceful Restart State	Indicates the graceful restart state. This feature is not supported in Multiprotocol BGP.
Advertised Restart Interval	Indicates the restart interval in seconds.
Forwarding State during restart	Indicates whether the peer has preserved the forwarding state during the graceful restart.
Activate IPv6 unicast	Indicates if the IPv6 unicast updates are enabled or not. Options include **enabled** or **disabled**.
Configured IPv6 NextHop Address	Specifies the IPv6 nexthop address. This is specified using the **ipv6 bgp neighbor ipv6-nexthop** command.
Neighbor Ipv6 unicast	Indicates whether Multiprotocol IPv6 Unicast capability is enabled or disabled between the peers.
BFD Status	Indicates whether BFD is enabled or disabled for this peer. The BFD status is configured through the **ip|ipv6 bgp neighbor bfd-state** command.
Activate IPv4 unicast	Indicates if the IPv4 unicast updates are enabled or not for this peer.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; BFD Status and Activate IPv4 unicast output fields added.
Release 8.4.1; ‘Neighbor TTL security’ output field added.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.
ip bgp neighbor ttl-security	Configures the Generalized TTL Security Mechanism (GTSM) for the BGP peer.

MIB Objects

```
alabgpMIBPeerGroup
   alaBgpPeerAddr
   alaBgpPeerAS
   alaBgpPeerPassive
   alaBgpPeerName
   alaBgpPeerMultiHop
   alaBgpPeerMaxPrefix
   alaBgpPeerMaxPrefixWarnOnly
   alaBgpPeerNextHopSelf
   alaBgpPeerTTLSecurityHops
   alaBgpPeerSoftReconfig
   alaBgpPeerInSoftReset
   alaBgpPeerIpv4Unicast
   alaBgpPeerIpv4Multicast
   alaBgpPeerRcvdRtRefreshMsgs
   alaBgpPeerSentRtRefreshMsgs
   alaBgpPeerRouteMapOut
   alaBgpPeerRouteMapIn
   alaBgpPeerLocalAddr
   alaBgpPeerLastDownReason
   alaBgpPeerLastDownTime
   alaBgpPeerLastReadTime
   alaBgpPeerRcvdNotifyMsgs
   alaBgpPeerSentNotifyMsgs
   alaBgpPeerLastSentNotifyReason
   alaBgpPeerLastRecvNotifyReason
   alaBgpPeerRcvdPrefixes
   alaBgpPeerDownTransitions
   alaBgpPeerType
   alaBgpPeerAutoReStart
   alaBgpPeerClientStatus
   alaBgpPeerConfedStatus
   alaBgpPeerRemovePrivateAs
   alaBgpPeerClearCounter
   alaBgpPeerTTL
   alaBgpPeerAspathListOut
   alaBgpPeerAspathListIn
   alaBgpPeerPrefixListOut
   alaBgpPeerPrefixListIn
   alaBgpPeerCommunityListOut
   alaBgpPeerCommunityListIn
   alaBgpPeerRestart
   alaBgpPeerDefaultOriginate
   alaBgpPeerReconfigureInBound
   alaBgpPeerReconfigureOutBound
   alaBgpPeerMD5Key
   alaBgpPeerMD5KeyEncrypt
   alaBgpPeerRowStatus
   alaBgpPeerUpTransitions
   alaBgpPeerLocalIntfName
   alaBgpPeerActivateIpv4
```

show ip bgp neighbors policy

Displays BGP peer policy information.

show ip bgp neighbors policy [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays all of the configured policies for the router, or the polices configured for a specific peer.

Examples

```
-> show ip bgp neighbors policy
Neighbor address  =  0.0.0.0,
  Neighbor autonomous system          = 1,
  Neighbor output policy map name     = <none>,
  Neighbor input policy map name      = <none>,
  Neighbor output aspath-list name    = <none>,
  Neighbor input aspath-list name     = <none>,
  Neighbor output prefix-list name    = <none>,
  Neighbor input prefix-list name     = <none>,
  Neighbor output community-list name = <none>,
  Neighbor input community-list name  = <none>,
  Neighbor soft reconfiguration       = enabled
  Neighbor output prefix6-list name   = <none>,
  Neighbor input prefix6-list name    = <none>
Neighbor address  =  0.0.0.1,
  Neighbor autonomous system          = 1,
  Neighbor output policy map name     = <none>,
  Neighbor input policy map name      = <none>,
  Neighbor output aspath-list name    = <none>,
  Neighbor input aspath-list name     = <none>,
  Neighbor output prefix-list name    = <none>,
  Neighbor input prefix-list name     = <none>,
  Neighbor output community-list name = <none>,
  Neighbor input community-list name  = <none>,
  Neighbor soft reconfiguration       = enabled
  Neighbor output prefix6-list name   = <none>,
  Neighbor input prefix6-list name    = <none>
```

output definitions

Neighbor autonomous system	The AS to which the peer is assigned. This can be assigned by using the **ip bgp neighbor remote-as** command.
Neighbor output policy map name	The outbound route map policy for the peer. This can be assigned by using the **ip bgp neighbor route-map** command.
Neighbor input policy map name	The inbound route map policy for the peer. This can be assigned by using the **ip bgp neighbor route-map** command.
Neighbor output aspath-list name	The outbound AS path list policy for the peer. This can be assigned by using the **ip bgp neighbor out-aspathlist** command.
Neighbor input aspath-list name	The inbound AS path list policy for the peer. This can be assigned by using the **ip bgp neighbor in-aspathlist** command.
Neighbor output prefix-list name	The outbound prefix list policy for the peer. This can be assigned by using the **ip bgp neighbor out-prefixlist** command.
Neighbor input prefix-list name	The inbound prefix list policy for the peer. This can be assigned by using the **ip bgp neighbor in-prefixlist** command.
Neighbor output community-list name	The outbound community list policy for the peer. This can be assigned by using the **ip bgp neighbor out-communitylist** command.
Neighbor input community-list name	The inbound community list policy for the peer. This can be assigned by using the **ip bgp neighbor in-communitylist** command.
Neighbor soft reconfiguration	Lists whether soft reconfigurations are enabled or disabled for this peer. This is configured using the **ip bgp neighbor soft-reconfiguration** command.
Neighbor output prefix6-list name	The outbound prefix6 list policy for the peer. This can be assigned by using the **ip bgp neighbor out-prefix6list** command.
Neighbor input prefix6-list name	The inbound prefix6 list policy for the peer. This can be assigned by using the **ip bgp neighbor in-prefix6list** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAS
   alaBgpPeerRouteMapOut
   alaBgpPeerRouteMapIn
   alaBgpPeerAspathListOut
   alaBgpPeerAspathListIn
   alaBgpPeerPrefixListOut
   alaBgpPeerPrefixListIn
   alaBgpPeerCommunityListOut
   alaBgpPeerCommunityListIn
   alaBgpPeerSoftReconfig
   alaBgpPeerPrefix6ListOut
   alaBgpPeerPrefix6ListIn
```

show ip bgp neighbors timer

Displays BGP peer timer statistics.

show ip bgp neighbors timer [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the timer values for all peer associated with this speaker, or for a specific peer.

Examples

```
-> show ip bgp neighbors timer
Legends: Nbr     = Neighbor
         As      = Autonomous System
         RtAdv   = Route Advertisement
         Kalive  = Keep Alive (actual)
         Ka(C)   = Configured Keep Alive
Nbr address     As    Hold  Hold(C) RtAdv Retry Kalive Ka(C)
---------------+-----+-----+-------+-----+-----+------+-----
192.40.4.29     3     90    90      30    120   30     30
192.40.4.121    5     0     90      30    120   0      30
```

output definitions

Nbr address	The IP address for this BGP peer. Assign this address through the **ip bgp neighbor** command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned through the **ip bgp neighbor remote-as** command.
Hold	The current count for the holdtime value.
Hold(C)	The holdtime value configured through the **ip bgp neighbor timers** command.
RtAdv	The route advertisement interval, in seconds, for updates between external BGP peers. This value is configured through the **ip bgp neighbor advertisement-interval** command.
Retry	The interval, in seconds, between retries by this peer to set up a connection through TCP with another peer. This value is configured through the **ip bgp neighbor timers** command.

output definitions (continued)

Kalive	The current count, in seconds, between keepalive messages. Keepalive messages do not contain route or status updates; they serve only to tell other peers that the connection is still live and this peer is reachable.
Ka(C)	The keepalive interval as configured through the **ip bgp neighbor timers** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

MIB Objects

N/A

show ip bgp neighbors statistics

Displays BGP peer message statistics.

show ip bgp neighbors statistics [*ip_address*]

Syntax Definitions

ip_address	A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays message statistics for all peers associated with this speaker, or with a specific peer.

Examples

```
-> show ip bgp neighbors statistics
Legends: RMSGS = number of received messages, SMSGS = number of sent messages
         RUPDS = number of Update messages received,
         SUPDS = number of Update messages sent,
         RNOFY = number of Notify messages received,
         SNOFY = number of Notify messages sent
         RPFXS = number of prefixes received
         UPTNS = number of UP transitions
         DNTNS = number of DOWN transitions

 Nbr address    As    RMSGS SMSGS RUPDS SUPDS RNOFY SNOFY RPFXS UPTNS DNTNS
---------------+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
192.40.4.29     3     110   123   5     0     0     1     8     2     2
192.40.4.121    5     0     0     0     0     0     0     0     0     0
```

output definitions

Nbr address	The IP address for this peer. This value is configured through the **ip bgp neighbor** command.
As	The autonomous system to which this peer belongs. This value is configured through the **ip bgp neighbor remote-as** command.
RMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.
SMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent by this peer.

output definitions (continued)

RUPDS	The number of route UPDATE messages received by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
SUPDS	The number of route UPDATE messages sent by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
RNOFY	The number of NOTIFY messages received by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
SNOFY	The number of NOTIFY messages sent by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
RPFXS	The number of unique route prefixes received by this peer.
UPTNS	The number of times this peer has come up, operationally.
DNTNS	Number of times this peer has gone down, operationally.

```
-> show ip bgp neighbors statistics 0.0.0.1
Neighbor address                  = 0.0.0.1,
# of UP transitions               = 0,
Time of last UP transition        = 00h:00m:00s,
# of DOWN transitions             = 0,
Time of last DOWN transition      = 00h:00m:00s,
Last DOWN reason                  = none,
# of msgs rcvd                    = 0,
# of Update msgs rcvd             = 0,
# of prefixes rcvd                = 0,
# of Route Refresh msgs rcvd      = 0,
# of Notification msgs rcvd       = 0,
Last rcvd Notification reason     = none [none]
Time last msg was rcvd            = 00h:00m:00s,
# of msgs sent                    = 0,
# of Update msgs sent             = 0,
# of Route Refresh msgs sent      = 0
# of Notification msgs sent       = 0,
Last sent Notification reason     = none [none]
Time last msg was sent            = 00h:00m:00s,
```

output definitions

Neighbor address	The IP address for this peer. This value is configured through the **ip bgp neighbor** command.
# of UP transitions	The number of times this peer has come up, operationally.
Time of last UP transition	The duration that this peer has been up.
# of DOWN transitions	Number of times this peer has gone down, operationally.
Time of last DOWN transition	The duration since this peer last went down.

output definitions (continued)

Last DOWN reason	Provides a message as the last reason why a peer went down. The possible reasons for going down are: user_request - user initiated conn_timeout - connection timer expired hold_timeout - hold timer expired bad_msg - received a bad message from neighbor fsm_blink - BGP FSM error peer_closed - neighbor closed connection peer_notify - neighbor sent fatal notification tcp_error - Fatal TCP error none - None
# of msgs rcvd	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received from this peer.
# of Update msgs rcvd	The number of route UPDATE messages received from this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of prefixes rcvd	The number of unique route prefixes received by this peer.
# of Route Refresh msgs rcvd	The number of route refresh requests this peer has received. Route refresh requests all routes learned be a peer.
# of Notification msgs rcvd	The number of NOTIFY messages received from this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last rcvd Notification reason	NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message received from this peer. The notification reasons are listed in two parts separated by a dash (-). The following are possible notification reasons: message header error - synchronization loss message header error - bad length message header error - bad type open message error - unsupported version open message error - bad peer autonomous system open message error - bad peer bgp id open message error - unsupported option open message error - authentication failure open message error - unacceptable hold time open message error - unsupported capability update message error - malformed attribute update message error - unknown attribute update message error - missing wellknown attribute update message error - attribute flags error update message error - attribute length error update message error - invalid origin update message error - as loop update message error - invalid nexthop update message error - optional attribute error update message error - invalid network update message error - malformed aspath cease - maximum number of prefixes reached cease - administrative shutdown cease - peer de-configured cease- administrative reset cease- connection rejected cease - other configuration change cease - connection collision resolution cease - out of resources hold time out - none fsm error - none none - none
Time last msg was rcvd	The duration since a message was received from this peer.
# of msgs sent	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent to this peer.
# of Update msgs sent	The number of route UPDATE messages sent to this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of Route Refresh msgs sent	The number of route refresh requests this peer has sent. Route refresh requests request all routes learned be a peer.
# of Notification msgs sent	The number of NOTIFY messages sent to this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last sent Notification reason	NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message sent by this peer. The notification reasons are listed in two parts separated by a dash (-). See the list of possible notification reasons under the description for the **Peer last received notification reason** field above.
Time last msg was sent	The duration since a message was sent to this peer.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Creates or deletes a BGP peer.

MIB Objects

N/A

show ip bgp policy aspath-list

Displays AS path list parameters.

show ip bgp policy aspath-list [*name***] [***"regular_expression"***]**

Syntax Definitions

name	An AS path name.
regular_expression	A regular expression. The regular expression must be enclosed by quotation marks.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command displays a list of all of the AS path policies for the router, or a single policy selected by the list name or regular expression.
- Regular expressions are defined in the **ip bgp policy aspath-list** command on page 29-108.
- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.

Examples

```
-> show ip bgp policy aspath-list
Aspath List Name          Aspath regular expression
------------------------+-------------------------------------------------
aspl1                     (500 | 400) ? 300$
aspl2                     (500 | 400)

-> show ip bgp policy aspath-list aspl1
Aspath List name = aspl1
Aspath Regexp    = (500 | 400) ? 300$
  Admin state      = disabled,
  Priority         = 1,
  Action           = deny,
  Primary index    = 0,
```

output definitions

Aspath List name	The name of the AS path list. This is defined using the **ip bgp policy aspath-list** command.
Aspath regular expression	The regular expression that defines the AS path list. This is defined using the **ip bgp policy aspath-list** command.

output definitions (continued)

Admin state	The administration state of the AS path policy. It is either enable or disable.
Priority	The AS path list priority. This is defined using the **ip bgp policy aspath-list priority** command.
Action	The AS path list action, either permit or deny. This is defined using the **ip bgp policy aspath-list action** command.
Primary index	The instance identifier for the AS path list. This value is not configurable.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy aspath-list	Creates or removes an AS path list.

MIB Objects

```
alabgpMIBAspathListGroup
   alaBgpAspathMatchListId
   alaBgpAspathMatchListRegExp
   alaBgpAspathMatchListPriority
   alaBgpAspathMatchListAction
   alaBgpAspathMatchListRowStatus
```

show ip bgp policy community-list

Displays community list parameters.

show ip bgp policy community-list [*name***] [***string***]**

Syntax Definitions

name	Community name.
string	A regular expression. The regular expression must be enclosed by quotation marks.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays a list of the community policies for the speaker, or a specific policy defined by its name or community match string.

Examples

```
-> show ip bgp policy community-list
Community list name       Community string
--------------------------+--------------------------------------------------
adfasdf                   0:0

-> show ip bgp policy community-list coml1
Community List name = coml1
Community string    = 600:1
  Admin state               = disabled,
  Match type                = exact,
  Priority                  = 1,
  Action                    = deny,
  Primary index             = 0
```

output definitions

Community List name	The community list name. This is defined using the **ip bgp policy community-list** command.
Community string	The community list definition. This is defined using the **ip bgp policy community-list** command.
Admin state	The administration state of the community list policy, either enabled or disabled.
Match type	The match type of the community list. This is defined using the **ip bgp policy community-list match-type** command.

output definitions (continued)

Priority	The community list priority. This is defined using the **ip bgp policy community-list priority** command.
Action	The community list action. This is defined using the **ip bgp policy community-list action** command.
Primary index	The instance identifier for the community list. This value is not configurable.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.

MIB Objects

```
alabgpMIBCommunityListGroup
   alaBgpCommunityMatchListId
   alaBgpCommunityMatchListString
   alaBgpCommunityMatchListPriority
   alaBgpCommunityMatchListType
   alaBgpCommunityMatchListAction
   alaBgpCommunityMatchListRowStatus
```

show ip bgp policy prefix-list

Displays prefix list parameters.

show ip bgp policy prefix-list [*name***] [***ip_address ip_mask***]**

Syntax Definitions

name	A prefix list name.
ip_address	A prefix list IP address.
ip_mask	An IP address mask.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the list of prefix-list policies configured for the speaker, or a specific list determined by the list name or IP address and mask.

Examples

```
-> show ip bgp policy prefix-list
Prefix List name          Prefix address  Prefix mask
-------------------------+---------------+--------------
pfxl1                     155.132.33.0    255.255.255.0
pfxl2                     155.148.32.0    255.255.255.0

-> show ip bgp policy prefix-list pfxl1
Prefix List name = pfxl1
Address          = 155.132.33.0
Mask             = 255.255.255.0
  Admin state        = disabled,
  Match Mask >= (GE) = 0,
  Match Mask <= (LE) = 0,
  Action             = deny
```

output definitions

Prefix List name	The name of the prefix list. This is defined using the **ip bgp policy prefix-list** command.
Address	The IP address of the prefix list. This is defined using the **ip bgp policy prefix-list** command.
Mask	The mask of the prefix list. This is defined using the **ip bgp policy prefix-list** command.
Admin state	The administrative state of the prefix list, either enabled or disabled.

output definitions (continued)

Match Mask >= (GE)	The GE match mask of the prefix list. This is defined using the **ip bgp policy prefix-list ge** command.
Match Mask <= (LE)	The GE match mask of the prefix list. This is defined using the **ip bgp policy prefix-list le** command.
Action	The action of the prefix list. This is defined using the **ip bgp policy prefix-list action** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alabgpMIBPrefixListGroup
   alaBgpPrefixMatchListId
   alaBgpPrefixMatchListAddr
   alaBgpPrefixMatchListMask
   alaBgpPrefixMatchListGE
   alaBgpPrefixMatchListLE
   alaBgpPrefixMatchListAction
   alaBgpPrefixMatchListRowStatus
```

show ip bgp policy prefix6-list

Displays prefix6 list parameters.

show ip bgp policy prefix6-list [*name***] [***ipv6_address/prefixLength***]**

Syntax Definitions

name	A prefix6 list name.
ip_address	A prefix6 list IPv6 address.
prefixLength	A prefix6 list prefix length.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the list of prefix6-list policies configured for the speaker, or a specific list determined by the list name or IPv6 address.

Examples

```
-> show ip bgp policy prefix6-list
Prefix6 List name      Prefix6 address/Prefix length
---------------------+------------------------------
p62                    ::/0
p63                    4001:1::/32

-> show ip bgp policy prefix6-list p63
Prefix6 List name = p63
Prefix          = 4001:1::
Prefix Length   = 32
Admin state        = enabled,
Match MaskLength >= (GE) = 32,
Match MaskLength <= (LE) = 0,
Action             = permit
```

output definitions

Prefix6 List name	The name of the prefix6 list. This is defined using the **ip bgp policy prefix6-list** command.
Prefix	The IPv6 address of the prefix6 list. This is defined using the **ip bgp policy prefix6-list** command.
Prefix Length	The prefix length of the prefix6 list. This is defined using the **ip bgp policy prefix6-list** command.
Admin state	The administrative state of the prefix6 list, either enabled or disabled.

output definitions (continued)

Match MaskLength >= (GE)	The GE match masklength of the prefix6 list. This is defined using the **ip bgp policy prefix6-list** command.
Match MaskLength <= (LE)	The LE match masklength of the prefix6 list. This is defined using the **ip bgp policy prefix6-list** command
Action	The action of the prefix6 list. This is defined using the **ip bgp policy prefix6-list** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	Creates or deletes a prefix6 match list.

MIB Objects

```
alaBgpPrefix6MatchListTable
   alaBgpPrefix6MatchListId
   alaBgpPrefix6MatchListAddr
   alaBgpPrefix6MatchListAddrLength
   alaBgpPrefix6MatchListGE
   alaBgpPrefix6MatchListLE
   alaBgpPrefix6MatchListAction
   alaBgpPrefix6MatchListRowStatus
```

show ip bgp policy route-map

Displays policy route map parameters.

show ip bgp policy route-map [*name***] [***sequence_number***]**

Syntax Definitions

name	Route map name.
sequence_number	A sequence number. The valid range is 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The route map is displayed as a summary table by entering only the route map name, or as a detailed list by specifying the sequence number.

Examples

```
-> show ip bgp policy route-map
RouteMap name             Instance
--------------------------+--------
rmap1                     1
rmap1                     2
rmap2                     1

-> show ip bgp policy route-map rmap1
RouteMap name     = rmap1
RouteMap instance = 1
  Admin state               = disabled,
  Local pref (mode/value)   = <none> / 0,
  Route map action          = permit,
  Origin                    = <none>,
  MED (mode/value)          = <none> / 0,
  Weight                    = 0,
  Aspath-List name          = aspl1,
  Aspath prepend            = <none>,
  Aspath match primitive    = 500 .* 400$,
  Prefix-List name          = <none>,
  Prefix match primitive    = 0.0.0.0 0.0.0.0,
  Prefix6-List name         = <none>,
  Prefix6 match primitive   = ::/0,
  Prefix6-List name         = <none>,
  Prefix6 match primitive   = ::/0,
  Community-List name       = coml2,
  Community match primitive = <none>,
  Community string [mode]   =  [Additive]
```

output definitions

RouteMap name	The name of the route map policy. This is determined using the **ip bgp policy prefix6-list** command.
RouteMap instance	The instance of the route map policy. This is determined using the **ip bgp policy prefix6-list** command.
Admin state	The administrative state of the route map policy, either enabled or disabled.
Local pref (mode/value)	The local preference of the route map policy. This is determined using the **ip bgp policy route-map lpref** command.
Route map action	The action of the route map policy. This is determined using the **ip bgp policy route-map action** command.
Origin	The origin of the route map policy. This is determined using the **ip bgp policy route-map origin** command.
MED (mode/value)	The MED of the route map policy. This is determined using the **ip bgp policy route-map med** command.
Weight	The weight of the route map policy. This is determined using the **ip bgp policy route-map weight** command.
Aspath-List name	The name of the AS path list attached to this route map.This is set using the **show ip bgp policy aspath-list** command.
Aspath prepend	The value to prepend to the AS_PATH attribute of the routes matched by this RouteMap instance (Empty quotes indicates no AS_PATH prepending is to be done).
Aspath match primitive	The regular expression used to match AS Path for this route map.
Prefix-List name	The name of the prefix list attached to this route map. This is set using the **show ip bgp policy prefix-list** command.
Prefix match primitive	The prefix to match for this route map.
Prefix6-List name	The name of the prefix6 list attached to this route map.
Prefix6 match primitive	The prefix6 to match for this route map.
Community-List name	The name of the community list attached to this route map. This is set using the **show ip bgp policy community-list** command.
Community match primitive	The community string to match for this route map.
Community string [mode]	The name of the community mode attached to this route map. This is set using the **ip bgp policy route-map community-mode** command.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; Prefix6-List name and Prefix6 match primitive output fields added.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alabgpMIBRouteMapGroup
   alaBgpRouteMapName
   alaBgpRouteMapInst
   alaBgpRouteMapAsPathMatchListId
   alaBgpRouteMapPrefixMatchListId
   alaBgpRouteMapCommunityMatchListId
   alaBgpRouteMapOrigin
   alaBgpRouteMapLocalPref
   alaBgpRouteMapLocalPrefMode
   alaBgpRouteMapMed
   alaBgpRouteMapMedMode
   alaBgpRouteMapAsPrepend
   alaBgpRouteMapSetCommunityMode
   alaBgpRouteMapCommunity
   alaBgpRouteMapMatchAsRegExp
   alaBgpRouteMapMatchPrefix
   alaBgpRouteMapMatchMask
   alaBgpRouteMapMatchCommunity
   alaBgpRouteMapWeight
   alaBgpRouteMapAction
   alaBgpRouteMapRowStatus
   alaBgpRouteMapPrefix6MatchListId
   alaBgpRouteMapMatchPrefix6
   alaBgpRouteMapMatchMaskLength6
```

ip bgp graceful-restart

Configures support for the graceful restart feature on a BGP router.

ip bgp graceful-restart

no ip bgp graceful-restart

Syntax Definitions

N/A

Defaults

Graceful restart is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable support for the graceful restart feature on a BGP router. It has only unplanned graceful restart.
- The minimum hardware configuration for this command is a redundant CMM configuration.
- Note that graceful restart does not support IPv6 prefixes at this time.

Examples

```
-> ip bgp graceful restart
-> no ip bgp graceful restart
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpGracefulRestart
   alaBgpRestartInterval
```

ip bgp graceful-restart restart-interval

Configures the grace period for achieving a graceful BGP restart.

ip bgp graceful-restart restart-interval [*seconds***]**

Syntax Definitions

seconds	The hitless restart timeout interval, in seconds. The valid range is 1–3600.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration.
- Note that graceful restart does not support IPv6 prefixes at this time.

Examples

```
-> ip bgp graceful-restart restart-interval 600
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpGracefulRestart
   alaBgpRestartInterval
```

ip bgp unicast

Enables or disables unicast IPv4 advertisements for the BGP routing process.

ip bgp unicast

no ip bgp unicast

Syntax Definitions

N/A

Defaults

By default, BGP IPv4 advertisements are enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to turn off IPv4 unicast advertisements.
- BGP should be disabled before enabling or disabling IPv4 unicast advertisements.
- IPv4 unicast advertisements may be turned off on homogeneous IPv6 networks that are not aware of IPv4 routing. In such cases, the command, **ip router router-id**, must be used to explicitly configure the 32-bit unique router identifier.

Examples

```
-> ip bgp unicast
-> no ip bgp unicast
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
alaBgpGlobal
   alaBgpMultiProtocolIpv4
```

ipv6 bgp unicast

Enables or disables unicast IPv6 advertisements for the BGP routing process.

ipv6 bgp unicast

no ipv6 bgp unicast

Syntax Definitions

N/A

Defaults

By default, IPv6 BGP advertisements are disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to turn off IPv6 unicast advertisements.
- BGP should be disabled before enabling or disabling IPv6 unicast advertisements.

Examples

```
-> ipv6 bgp unicast
-> no ipv6 bgp unicast
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp unicast	Enables or disables unicast IPv4 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
   alaBgpMultiProtocolIpv6
```

ip bgp neighbor activate-ipv6

Enables or disables the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv4 addresses.

ip bgp neighbor *ip_address* **activate-ipv6**

no ip bgp neighbor i*p_address* **activate-ipv6**

Syntax Definitions

ip_address	The 32-bit IPv4 address of the neighbor.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to disable the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv4 addresses.

Examples

```
-> ip bgp neighbor 1.0.0.1 activate-ipv6
-> no ip bgp neighbor 1.0.0.1 activate-ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp neighbors	Displays BGP peer main status.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerIpv6Unicast
```

ip bgp neighbor ipv6-nexthop

Configures the IPv6 next hop addresses for the IPv6 prefixes advertised between BGP peers. These BGP peers are identified by their IPv4 addresses.

ip bgp neighbor *ip_address* **ipv6-nexthop** *ipv6_address*

Syntax Definitions

ip_address	The 32-bit IPv4 address of the neighbor.
ipv6_address	A 128-bit global IPv6 address to be used as the next hop for IPv6 routes being advertised to this BGP speaker.

Defaults

By default, the IPv6 next hop value is set to all zeros.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- To reset the IPv6 next hop value, enter an all-zero address.
- For internal BGP (IBGP) peers, the IPv6 next hop is used only if the peer **next-hop-self** option is configured.
- For external BGP (EBGP) peers, the IPv6 next hop is used for all the advertised IPv6 routes.

Examples

```
-> ip bgp neighbor 1.0.0.1 ipv6-nexthop 2001:100:3:4::1
-> ip bgp neighbor 1.0.0.1 ipv6-nexthop ::
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeerTable
   alaBgpPeerAddr
   alaBgpPeerIpv6NextHop
```

show ipv6 bgp path

Displays the known IPv6 BGP paths for all the routes or a specific route.

show ipv6 bgp path [ipv6-addr *ipv6_address/prefix_length***] [detail]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

By default, IPv6 BGP paths for all the routes will be displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ipv6_address/prefix_length* parameter to display the IPv6 BGP paths for a specified route.
- 'Detail' option when used displays the AS Path details of each route.

Examples

```
-> show ipv6 bgp path
Legends: Sta     = Path state
         >       = best, F = feasible, S = stale
         U       = un-synchronized
         Nbr     = Neighbor
         (O)     = Path Origin (? = incomplete, i = igp, e = egp)
         degPref = degree of preference
Sta  Prefix                       Nbr Address                          (O) degPref
---+-----------------------------+------------------------------------+---+-------
 >  2020:100:200:1::/64          2001:100:3:4::1                       i   100
 >  2020:100:200:2::/64          2001:100:3:4::1                       i   100
 >  2020:100:200:3::/64          2001:100:3:4::1                       i   100
 >  2020:100:200:4::/64          2001:100:3:4::1                       i   100
 >  2020:100:200:5::/64          2001:100:3:4::1                       i   100
 >  2525:2525:1::/48             100.3.4.1                             i   100
 >  2525:2525:2::/48             100.3.4.1                             i   100
 >  2525:2525:3::/48             100.3.4.1                             i   100
 >  2525:2525:4::/48             100.3.4.1                             i   100
 >  2525:2525:5::/48             100.3.4.1                             i   100

-> show ipv6 bgp path detail
Legends: Sta     = Path state
         >       = best, F = feasible, S = stale
         Nbr     = Neighbor
         (O)     = Path Origin (? = incomplete, i = igp, e = egp)
         degPref = degree of preference
```

```
Sta  Prefix            Nbr address               degPref AS Path, (O)
---+-----------------+-------------------------+-------+-----------------
 >  3001:1::/64         2001:1::2                 100     65535 65530, i
 >  3001:1:0:1::/64     2001:1::2                 100     65535 65530, i
 >  3001:1:0:2::/64     2001:1::2                 100     65535 65530, i
 >  4001:1:0:1::/64     2101::51                  140     65536, i
 >  4001:1:0:2::/64     2101::51                  140     65536, i
 >  4001:1:0:3::/64     2101::51                  140     65536, i
```

output definitions

Sta	Status flag. A greater-than sign (>) indicates this is the best route to the destination.
Prefix	The destination address of the IPv6 route in the hexadecimal format.
Nbr Address	The IP or IPv6 address of the BGP peer that advertises this path.
(0)	The origin attribute of this route path. A question mark (**?**) indicates incomplete, and **i** indicates IGP, and an **e** indicates EGP.
degPref	The local preference value assigned to this route path.

```
-> show ipv6 bgp path ipv6-addr 2020:100:200:1::/64
BGP Path parameters
Path address   = 2020:100:200:1::
Path Length    = 64
Path protocol  = ibgp
Path neighbor  = peer(2001:100:3:4::1)
  Path nextHop            = 2001:100:3:4::1,
  Path origin             = igp,
  Path local preference   = 100,
  Path state              = active,
  Path weight             = 0,
  Path preference degree  = 100,
  Path autonomous systems = [nAs=0] : <none>,
  Path MED                = <none>,
  Path atomic             = no,
  Path AS aggregator      = <none>,
  Path IPaddr aggregator  = <none>,
  Path community          = <none>,
  Path Originator Id      = <none>,
  Path Cluster List       = <none>,
  Path unknown attribute  = <none>
```

output definitions

Path address	The IPv6 address for route path.
Path Length	The prefix length of the IPv6 path.
Path protocol	The protocol from which this route path was learned. Possible values for this field are as follows: **local**, **static**, **directhost**, **rip**, **ospf**, **isis**, **ibgp**, **ebgp**, and **other**.
Path neighbor	The IPv6 address of the BGP peer.
Path nextHop	The next hop along the route path.
Path origin	The BGP origin attribute. Possible values will be **igp**, **egp**, **incomplete**, and **none**. The origin attribute is considered during the route decision process.

output definitions (continued)

Path local preference	The local preference value for this route as received in an UPDATE message. A negative value (for example, the **-1** in the above display) indicates that the local preference value is missing for this route path.
Path state	Indicates the state of the path.The possible states are **best**, **feasible**, **policy-wait**, **un-synchronized**, **dampened**, or **none**. When path state is **none**, it indicates that there are no paths to this prefix and the route is being purged from the system.
Path weight	The path weight as assigned through inbound and outbound policies.
Path preference degree	The local preference assigned to this route through an inbound or outbound policy, or, if the local preference value is missing, the default local preference (which is assigned through the **ip bgp default local-preference**).
Path autonomous systems	The AS path for this route. These numbers show the ASs through which the route has traversed with the most recent AS listed first. In the above example, this route began its path in AS 2 and then traveled through AS 3.
Path MED	The multi-exit discriminator (MED) value for this route path. A negative value (for example, the **-1** in the above display) indicates that the MED value is missing for this route path.
Path atomic	Indicates whether the ATOMIC-AGGREGATE attribute has been set for this route. When set (this field would read **yes**), this attribute indicates that an aggregate has caused a loss of information for this route (a less specific route was chosen over a more specific route included in the aggregate).
Path AS aggregator	Part of the AGGREGATOR attribute. This field indicates the AS for the BGP speaker that created the aggregate. A value of **<none>** indicates this is not an aggregate route.
Path IPaddr aggregator	Part of the AGGREGATOR attribute. This field indicates the IP address for the BGP speaker that created the aggregate. A value of **<none>** indicates that this is not an aggregate route.
Path community	Indicates the community to which this route path belongs, if applicable. A value of **<none>** indicates that this route does not belong to a community.
Path Originator Id	The Router Id of the BGP4 speaker that performed route reflection
Path Cluster List	Sequence of Cluster Id values representing the reflection path that the route has passed, if this is a reflected route in the local AS.
Path unknown attribute	Indicates BGP attributes found in UPDATE messages which the router does not support. For example, multi-protocol attributes are not supported by the router in this release, but it is possible for these attributes to appear in a BGP route.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; ‘detail’ keyword added.

Related Commands

show ipv6 bgp routes	Displays the known IPv6 BGP routes.

MIB Objects

```
alaBgpPath6Table
   alaBgpPath6Addr
   alaBgpPath6MaskLen
   alaBgpPath6PeerBgpId
   alaBgpPath6SrcProto
   alaBgpPath6Weight
   alaBgpPath6Pref
   alaBgpPath6State
   alaBgpPath6Origin
   alaBgpPath6NextHop
   alaBgpPath6As
   alaBgpPath6LocalPref
   alaBgpPath6Med
   alaBgpPath6Atomic
   alaBgpPath6AggregatorAs
   alaBgpPath6AggregatorAddr
   alaBgpPath6Community
   alaBgpPath6OriginatorId
   alaBgpPath6ClusterList
   alaBgpPath6PeerName
   alaBgpPath6UnknownAttr
```

show ipv6 bgp routes

Displays the known IPv6 BGP routes.

show ipv6 bgp routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 bgp routes
Legends: ECL = EBGP change list, ICC = IBGP client change list
         ICL = IBGP change list, LCL = local change list
         AGG = Aggregation, AGC = Aggregation contribution
         AGL = Aggregation list, GDL = Deletion list
         AGW = Aggregation waiting, AGH = Aggregation hidden
         DMP = Dampening, ACT = Active route
 Prefix                          ECL ICC ICL LCL AGG AGC AGL AGW AGH GDL DMP ACT
--------------------------------+---+---+---+---+---+---+---+---+---+---+---+----
 2020:100:200:1::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2020:100:200:2::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2020:100:200:3::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2020:100:200:4::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2020:100:200:5::/64             No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:1::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:2::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:3::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:4::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
 2525:2525:5::/48                No  No  No  No  No  No  No  No  No  No  No  Yes
```

output definitions

Prefix	The destination address of the IPv6 route in the hexadecimal format.
ECL	External BGP change list. When Yes, this route will be advertised as soon as the route advertisement timer expires.
ICC	Internal BGP client change list. When Yes, this route will be advertised to internal non-clients.

output definitions (continued)

ICL	Internal BGP change list. When Yes, this route has changes that need to be advertised.
LCL	Local change list. When Yes, this route is local.
AGG	Aggregation. When Yes, this route is an aggregate route.
AGC	Aggregation contribution. When Yes, this route is part of an aggregate route.
AGL	Aggregation list. When Yes, this route is placed on an aggregate list.
AGW	Aggregation waiting. When Yes, this route is waiting for an aggregate contributor.
AGH	Aggregation hidden. When Yes, this route is hidden as part of an aggregate route.
GDL	Deletion list. When Yes, this route will be deleted.
DMP	Dampening. Indicate whether this route has been dampened. If 'Yes', then this route has been dampened and a dampening history exists.
ACT	Active route. When Yes, the route is active.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp path	Displays the known IPv6 BGP paths for all the routes or a specific route.

MIB Objects

```
alaBgpRoute6Table
   alaBgpRoute6Addr
   alaBgpRoute6MaskLen
   alaBgpRoute6State
   alaBgpRoute6IsHidden
   alaBgpRoute6IsAggregate
   alaBgpRoute6IsAggregateContributor
   alaBgpRoute6IsAggregateList
   alaBgpRoute6IsAggregateWait
   alaBgpRoute6IsOnEbgpChgList
   alaBgpRoute6IsOnIbgpClientChgList
   alaBgpRoute6IsOnIbgpChgList
   alaBgpRoute6IsOnLocalChgList
   alaBgpRoute6IsOnDeleteList
   alaBgpRoute6IsDampened
```

ipv6 bgp network

Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

ipv6 bgp network *ipv6_address/prefix_length*

no ipv6 bgp network *ipv6_address/prefix_length*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to turn off the advertisement of locally reachable IPv6 networks.

Examples

```
-> ipv6 bgp network 2001::1/64
-> no ipv6 bgp network 2001::1/64
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp network admin-state	Enables or disables a BGP network.
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
```

ipv6 bgp network community

Defines a community for a route created by the **ipv6 bgp network** command. Communities are a way of grouping BGP peers that do not share an IPv6 subnet or an AS.

ipv6 bgp network *ipv6_address/prefix_length* **[community {none | no-export | no-advertise | no-export-subconfed |** *num* **|** *num:num***}]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask). The valid range is 3–128
none	Removes a prefix from a community.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
num	The community attribute number.
num:num	Community attribute in the AS:NN format. AS indicates the autonomous system and NN indicates the community number.

Defaults

By default, a route is not assigned to a community.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **community** attribute is defined.
- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.

Examples

```
-> ipv6 bgp network 2004::2/64 community 23:20
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to **community** string.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6Community
```

ipv6 bgp network local-preference

Defines the local preference value for a route generated by the **ipv6 bgp network** command. This value will override the default local preference value; it is used when announcing this network to internal peers.

ipv6 bgp network *ipv6_address/prefix_length* **[local-preference** *num***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).
num	The local preference attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
num	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **local-preference** attribute is defined.

Examples

```
-> ipv6 bgp network 2004::1/24 local-preference 6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6LocalPref
```

ipv6 bgp network metric

Configures the Multi-Exit Discriminator (MED) attribute value for an network generated by the **ipv6 bgp network** command. This value is sent from routers of one AS to another to indicate the path that the remote AS can use to send data to the local AS.

ipv6 bgp network *ipv6_address/prefix_length* **[metric** *num***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).
num	The MED attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
num	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **metric** attribute is defined for the same route.

Examples

```
-> ipv6 bgp network 2001::1/64 metric 20
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as a IPv6 BGP network to other BGP peers.
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6Metric
```

ipv6 bgp network admin-state

Enables or disables a BGP network. The BGP status must be manually enabled after configuring all the BGP neighbor and network parameters.

ipv6 bgp network *ipv6_address/prefix_length* **[admin-state {enable | disable}]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).
enable	Enables the BGP network.
disable	Disables the BGP network.

Defaults

By default, the BGP network is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **status** attribute is defined.

Examples

```
-> ipv6 bgp network 2001::1/64 admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6RowStatus
```

show ipv6 bgp network

Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

show ipv6 bgp network [*ipv6_address/prefix_length***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.
/prefix_length	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

By default, all IPv6 BGP networks and their status will be displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the *ipv6_address/prefix_length* parameter to display the status of a specific IPv6 BGP network.

Examples

```
show ipv6 bgp network
 Network                            Admin state Oper state
-----------------------------------+-----------+----------
2525:500:600::/64                   enabled     active


show ipv6 bgp network 2525:500:600::/64
Network address          = 2525:500:600::/64,
Network admin state      = enabled,
Network oper state       = active,
Network metric           = 0,
Network local preference = 0,
Network community string = <none>
```

output definitions

Network or **Network address**	The IPv6 address configured for this local BGP network. This value is configured through the **ipv6 bgp network** command.
Admin state or **Network admin state**	Indicates whether this local BGP network is administratively enabled or disabled. This value is configured through the **ipv6 bgp network admin-state** command.
Oper state or **Network oper state**	Indicates whether this BGP local network is operationally active or inactive.

output definitions (continued)

Network metric	The multi-exit discriminator (MED) value configured for this local BGP network. This value is configured through the **ipv6 bgp network metric** command.
Network local preference	The local preference value for this local BGP network. This value is configured through the **ipv6 bgp network local-preference** command.
Network community string	The community string value for this local BGP network. This value is configured through the **ipv6 bgp network community** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp network	.Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

MIB Objects

```
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6State
   alaBgpNetwork6Metric
   alaBgpNetwork6LocalPref
   alaBgpNetwork6Community
   alaBgpNetwork6RowStatus
```

ipv6 bgp neighbor

Creates or deletes a BGP peer relationship using IPv6 addresses.

ipv6 bgp neighbor *ipv6_address*

no ipv6 bgp neighbor *ipv6_address*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the new BGP peer.

Defaults

By default, no BGP peers are configured in the BGP network.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a BGP peer.
- To establish a BGP session, the BGP peer should be reachable.
- You must manually enable a BGP peer after creating it. A BGP peer is enabled using the **ipv6 bgp neighbor admin-state** command.
- Once created, a BGP peer must be assigned an autonomous system number using the **ipv6 bgp neighbor remote-as** command.
- Use **update-source** keyword to configure the IPv6 interface when link-local address is used as neighbor address.

Examples

```
-> ipv6 bgp neighbor 2001::1
-> no ipv6 bgp neighbor 2001::1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp neighbor admin-state	Enables or disables the BGP peer status.
ipv6 bgp neighbor remote-as	Assigns an AS number to the BGP peer.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
```

ipv6 bgp neighbor ttl-security

Configures the Generalized TTL Security Mechanism (GTSM) for the BGP peer. GTSM allows to set the maximum number of hops for the IP packets between the switch and the peer. If the maximum number of hops exceeds, the packet is dropped at the NI.

ipv6 bgp neighbor *ipv6_address* **ttl-security** *num*

ipv6 bgp neighbor *ipv6_address* **no ttl-security**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
num	The maximum number of hops between the switch and the peer. The valid range for GTSM is 0 to 255.

Defaults

By default GTSM is disabled for communication with the peer.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- GTSM must be manually enabled on both peers in a connection.
- When GTSM is enabled, eBGP multihop must be disabled or vise-versa.
- Use the **no** form of this command to disable GTSM.

Examples

```
-> ipv6 bgp neighbor 2001::1 ttl-security 6
-> ipv6 bgp neighbor 2001::1 no ttl-security
```

Release History

Release 8.4.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6TTLSecurityHops
```

ipv6 bgp neighbor activate-ipv4

Enables the advertisement of IPv4 unicast capability to the IPv6 BGP peer.

ipv6 bgp neighbor *ipv6_address* **[activate-ipv4]**

no ipv6 bgp neighbor i*pv6_address* **[activate-ipv4]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the new BGP peer.
activate-ipv4	Enable the advertisement of IPv4 unicast capability to the IPv6 BGP peer.

Defaults

By default, the command is enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to disable the advertisement of IPv4 unicast capability to IPv6 BGP peer.

Examples

```
-> ipv6 bgp neighbor 2001::1 activate-ipv4
-> no ipv6 bgp neighbor 2001::1 activate-ipv4
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor	Creates or deletes a BGP peer relationship using IPv6 addresses.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ActivateIpv4
```

ipv6 bgp neighbor activate-ipv6

Enables the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* **[activate-ipv6]**

no ipv6 bgp neighbor i*pv6_address* **[activate-ipv6]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to disable the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv6 addresses.

Examples

```
-> ipv6 bgp neighbor 1.0.0.1 activate-ipv6
-> no ipv6 bgp neighbor 1.0.0.1 activate-ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ActivateIpv6
```

ipv6 bgp neighbor ipv6-nexthop

Configures the IPv6 next hop addresses for IPv6 prefixes advertised between BGP peers. These BGP peers are identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* **[ipv6-nexthop** *ipv6_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the next hop router.

Defaults

By default, the IPv6 next hop address is set to all zeros.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- To reset the IPv6 next hop value, enter an all-zero address.
- For internal BGP (IBGP) peers, the IPv6 next hop is used only if the peer **next-hop-self** option is configured.
- For external BGP (EBGP) peers, the IPv6 next hop is used for all the advertised IPv6 routes.
- For BGP peers configured with their link-local addresses, the configured IPv6 next hop is used while advertising IPv6 prefixes.

Examples

```
-> ipv6 bgp neighbor 2001::1 ipv6-nexthop fe80::/24
-> no ipv6 bgp neighbor 2001::1 ipv6-nexthop fe80::/24
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeerIpv6NextHop
```

ipv6 bgp neighbor admin-state

Enables or disables the BGP peer status. These peers are identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* **[admin-state {enable | disable}]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the new BGP peer.
enable	Enables the BGP peer.
disable	Disables the BGP peer.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- You should first create a BGP peer and assign it an IPv6 address using the **ipv6 bgp neighbor** command before enabling the peer.
- You should configure all the BGP peer related commands before enabling a BGP peer. Once you have enabled the peer, it will begin sending BGP connection and route advertisement messages.

Examples

```
-> ipv6 bgp neighbor 2001::1 admin-state enable
-> ipv6 bgp neighbor 2001::1 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6RowStatus
```

ipv6 bgp neighbor clear

Restarts the IPv6 BGP peer. The peer will be unavailable during this restart.

ipv6 bgp neighbor *ipv6_address* **clear**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command whenever changes occur to BGP-related access lists, weights, distribution lists, timer specifications, or administrative distance.
- Many peer commands restart the peer as soon as they are configured. The following commands restart the BGP peer for which they are configured:
  - **ipv6 bgp neighbor remote-as**
  - **ipv6 bgp neighbor md5 key**
  - **ipv6 bgp neighbor passive**
  - **ipv6 bgp neighbor ebgp-multihop**
  - **ipv6 bgp neighbor maximum-prefix**
  - **ipv6 bgp neighbor update-source**
  - **ipv6 bgp neighbor next-hop-self**
  - **ipv6 bgp neighbor soft-reconfiguration**
  - **ipv6 bgp neighbor route-reflector-client**
  - **ip bgp confederation neighbor6**
  - **ipv6 bgp neighbor remove-private-as**
  - **ipv6 bgp neighbor update-source-address**
- You do not need to issue the **ipv6 bgp neighbor clear** command after issuing any of the above commands.

Examples

```
-> ipv6 bgp neighbor 2001::1 clear
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor auto-restart	Automatically attempts to restart a BGP peer session after a session terminates.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Restart
```

ipv6 bgp neighbor auto-restart

Enables or disables BGP peer automatic restart. When enabled, this IPv6 peer will automatically attempt to restart a session with another peer after a session with that peer terminates. When disabled, this peer will not try to re-establish a session with another peer after the session terminates; in such a case, the other peer will have to restart the session for the two peers to resume communication.

ipv6 bgp neighbor *ipv6_address* **auto-restart**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the neighbor.

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable automatic peer restart.
- After a session with another peer terminates, the local BGP speaker will wait 60 seconds before attempting to restart the session. If the session does not start on the first attempt a second attempt will be made after another 120 seconds (60x2). On each unsuccessful session attempt, the previous delay between restarts is multiplied by 2, up to a maximum delay of 240 seconds. An exception to this rule occurs when the peer session terminates on receipt of a NOTIFY message with 'unsupported option' code or 'unsupported capability' code; in these cases the delay between restart attempts will begin at 1 second and multiply by 2 after each unsuccessful restart attempt (up to a maximum of 240 second delay).
- Disabling this option can be helpful in cases where other peers are prone to frequent flapping or sending many NOTIFY messages. By not restarting sessions with unstable neighbors, the local BGP speaker forces those unstable neighbors to re-initialize the connection.

Examples

```
-> ipv6 bgp neighbor 2001::1 auto-restart
-> no ipv6 bgp neighbor 2001::1 auto-restart
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor	Creates or deletes a BGP peer relationship using IPv6 addresses.
ipv6 bgp neighbor admin-state	Enables or disables the BGP peer status.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6AutoRestart
```

ipv6 bgp neighbor remote-as

Assigns an AS number to the BGP peer.

ipv6 bgp neighbor *ipv6_address* **[remote-as** *value***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
value	Autonomous system number in the asplain, asdot+, or asdot formats.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A BGP peer created with the **ipv6 bgp neighbor** command cannot be enabled until it is assigned an autonomous system number. If the AS number assigned to the peer matches the AS number of the local BGP speaker (assigned using the **ip bgp autonomous-system** command), the peer is considered internal to the local autonomous system. Otherwise, the peer is considered external to the local BGP speaker's AS.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::1 remote-as 100
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; modified the command.

Related Commands

ip bgp autonomous-system	Sets the AS for the local BGP speaker.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6AS
```

ipv6 bgp neighbor timers

Configures the KEEPALIVE message interval and hold time interval (in seconds) with regards to the specified BGP peer.

ipv6 bgp neighbor *ipv6_address* **[timers** *num num***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.
num	The KEEPALIVE message interval in seconds.
num	The hold time interval in seconds.

Defaults

parameter	default
num (keepalive)	30 seconds
num (holdtime)	90 seconds

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- KEEPALIVE messages do not contain route updates or indicate a change in the status of the BGP peer; they indicate to the receiving BGP peer that the connection is still live and the peer is reachable.
- By default, the KEEPALIVE interval of 30 seconds is one-third the default hold time interval of 90 seconds. The KEEPALIVE interval can never be more than one-third the value of the hold time interval. When the hold time interval is reached without receiving KEEPALIVE or other updates messages, the peer is considered dead.
- Setting the KEEPALIVE value to zero means no KEEPALIVE messages will be sent.
- Once a connection is established with a peer and a time period of the length specified in this command transpires with no messages from the remote peer, then the connection with that remote peer will be considered dead.
- The hold timer is used during the connection setup process and for on-going connection maintenance with BGP peers. If the peer does not receive a KEEPALIVE, UPDATE, or NOTIFICATION message within this time period, then the BGP connection will be closed.
- Both the KEEPALIVE and hold time interval should be set at the same time.
- Using this command without the variables resets the variables to their default value.

Examples

```
-> ipv6 bgp neighbor 2001::1 timers 80 240
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp neighbor conn-retry-interval	The interval, in seconds, between BGP retries to set up a connection with another peer through the transport protocol.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6HoldTime
   alaBgpPeer6KeepAlive
```

ipv6 bgp neighbor maximum-prefix

Configures the maximum number of prefixes, or paths, the local router can receive from a BGP peer in UPDATE messages.

ipv6 bgp neighbor *ipv6_address* **[maximum-prefix** *num* **[warning-only]]**

no ipv6 bgp neighbor *ipv6_address* **[maximum-prefix** *num* **[warning-only]]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.
num	The number of prefixes. The valid range is 0–4294967295.

Defaults

parameter	default
num	5000

By default, **warning-only** is enabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the number of prefixes sent by the BGP peer reaches the maximum limit, the peer is restarted.
- You can use BGP logging to receive a warning when the number of prefixes received from the peer reaches 80 percent of the value you configure in this command.
- If the **warning-only** prefix is used, the operator will be warned when the peer exceeds 80 percent of the configured number of maximum prefixes.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::2 maximum-prefix 1000 warning-only
-> no ipv6 bgp neighbor 2001::2 maximum-prefix 1000
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6MaxPrefix
   alaBgpPeer6MaxPrefixWarnOnly
```

ipv6 bgp neighbor next-hop-self

Configures router to advertise its peering address as the next hop address for the specified neighbor.

ipv6 bgp neighbor *ipv6_address* **[next-hop-self]**

no ipv6 bgp neighbor *ipv6_address* **[next-hop-self]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.

Defaults

By default, the **next-hop-self** parameter of BGP updates is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the **next-hop-self** parameter.
- In meshed networks, the BGP peer may not have direct connections to other peers. When such a peer receives route updates from these distant peers (through other peers), it may treat the remote peer as if it were the next hop in the routing path. Packet forwarding will not work in such a case because no direct connection exists. This command allows the peer to deem itself the next hop on the routing path so that the two non-connected peers can route packets. This peer would have a direct connection to both peers that want to exchange packets.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::2 next-hop-self
-> no ipv6 bgp neighbor 2001::2 next-hop-self
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6NextHopSelf
```

ipv6 bgp neighbor conn-retry-interval

The interval, in seconds, between BGP retries to set up a connection with another peer through the transport protocol. In the connect state, BGP tries to set up a connection with a remote peer. If the connection fails, then the connection retry interval starts. Once this interval elapses, BGP retries setting up the connection.

ipv6 bgp neighbor *ipv6_address* **[conn-retry-interval** *num***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP neighbor.
num	The time interval (in seconds) between retries. The valid range is 0–65535.

Defaults

parameter	default
num	120

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The connection retry time interval starts when a connection to a peer is lost.
- Using this command without the *num* variable resets the variable to its default value.

Examples

```
-> ipv6 bgp neighbor 2001::2 conn-retry-interval 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ConnRetryInterval
```

ipv6 bgp neighbor default-originate

Enables or disables the BGP local speaker to advertise a default route to the peer.

ipv6 bgp neighbor *ipv6_address* **[default-originate]**

no ipv6 bgp neighbor *ipv6_address* **[default-originate]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the neighbor.

Defaults

This **default-originate** parameter is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the BGP peer default origination.
- When this command is enabled, the local BGP speaker advertises the default route to the peer. Such a default route overrides any learned default (propagation) and outbound policy. The default route `::/0` does not need to exist on the local router.
- If the peer is capable of exchanging IP as well as IPv6 prefixes, the default route for both IP and IPv6 is advertised.

Examples

```
-> ipv6 bgp neighbor 2001::1 default-originate
-> no ipv6 bgp neighbor 2001::1 default-originate
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6DefaultOriginate
```

ipv6 bgp neighbor update-source

Configures the local IPv6 interface from which a BGP peer will be connected. This local IPv6 interface can be configured for internal and external BGP peers.

ipv6 bgp neighbor *ipv6_address* **[update-source** *interface_name***]**

no ipv6 bgp neighbor *ipv6_address* **[update-source** *interface_name***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.
interface_name	The name of the local IPv6 interface that provides the TCP connection for this BGP peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The BGP peer is restarted after issuing this command.
- If a BGP peer is configured with its link-local address, use the **update-source** parameter to specify the name of the IPv6 interface from which this peer is reachable. This is required to establish a BGP peering session.

Examples

```
-> ipv6 bgp neighbor 2004::1 update-source bgp_ipv6
-> no ipv6 bgp neighbor 2004::1 update-source bgp_ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.
ipv6 interface	Configures an IPv6 interface on a VLAN or IPv6 tunnel.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6LocalIntfName
```

ipv6 bgp neighbor ipv4-nexthop

Configures the IPv4 next hop addresses for IPv4 prefixes advertised between BGP peers. These BGP peers are identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* **[ipv4-nexthop** *ip_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.
ip_address	The 32-bit IP address of the next hop.

Defaults

By default, the IPv4 next hop value is set to all zeros.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

To reset the IPv4 next hop value, enter an all-zero address.

Examples

```
-> ipv6 bgp neighbor 2004::1 ipv4-nexthop 172.22.2.115
-> ipv6 bgp neighbor 2004::1 ipv4-nexthop 0.0.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors .Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6Ipv4NextHop
```

ipv6 bgp neighbor advertisement-interval

Configures the time interval for updates between external IPv6 BGP peers.

ipv6 bgp neighbor *ipv6_address* **advertisement-interval** *value*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the neighbor.
value	An advertisement time interval in seconds. The valid range is 0–65535.

Defaults

parameter	default
value	30

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Internal peers sharing the same AS as the local BGP speaker (configured in the **ip bgp autonomous-system**command) use the global route advertisement update interval. This command sets the interval this peer uses to send BGP UPDATE messages to external IPv6 BGP peers.

Examples

```
-> ipv6 bgp neighbor 2001::1 advertisement-interval 60
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show ipv6 bgp neighbors	.Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6MinRouteAdvertisementInterval
```

ipv6 bgp neighbor description

Configures the IPv6 BGP Peer name.

ipv6 bgp neighbor *ipv6_address* **description** *string*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the neighbor.
string	Peer name (1 - 20 characters).

Defaults

parameter	default
string	peer (ipv6_address)

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The peer name is a text identifier that, by default, follows the format "peer(ipv6-address)" where ipv6-address is the IPv6 address of the BGP peer. For example, the default name of an IPv6 BGP peer at address 2001::1 would be “peer(2001::1)”.
- A peer name with embedded spaces must be enclosed in quotation marks.

Examples

```
-> ipv6 bgp neighbor 2001::1 description "peer6 for building 3"
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor	Creates or deletes a BGP peer relationship using IPv6 addresses.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6Name
```

ipv6 bgp neighbor ebgp-multihop

Allows external IPV6 BGP peers to communicate with each other even when they are not directly connected. The absence of communication between disconnected peers can occur when a router that is not running BGP sits between two BGP speakers; in such a scenario the BGP speakers are multiple hops from each other. By enabling this command, you allow the IPv6 BGP peers to speak to each other despite the non-BGP router that sits between them.

ipv6 bgp neighbor *ipv6_address* **ebgp-multihop [***ttl***]**

no ipv6 bgp neighbor *ipv6_address* **ebgp-multihop**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
ttl	The Time to Live for the multi-hop connection, in seconds. The range is 1 to 255.

Defaults

parameter	default
ttl	255

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable multi-hop connections.
- By default an external IPv6 BGP peer is on a directly connected subnet. This command allows you to configure an external IPv6 BGP peer that is not directly connected and may be multiple hops away. It should be used with caution and only with the guidance of qualified technical support.
- The BGP peer is restarted after issuing this command.
- When eBGP multihop is enabled, GTSM must be disabled or vise-versa.

Examples

```
-> ipv6 bgp neighbor 2001::1 ebgp-multihop
-> ipv6 bgp neighbor 2001::1 ebg-multihop 50
-> no ipv6 bgp neighbor 2001::1 ebgp-multihop
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor	Creates or deletes a BGP peer relationship using IPv6 addresses.
ipv6 bgp neighbor next-hop-self	Configures router to advertise its peering address as the next hop address for the specified neighbor.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6MultiHop
```

ipv6 bgp neighbor update-source-address

Configures the local IPv6 address from which a BGP peer will be connected if the peer is configured with its link-local address. This local IPv6 address can be configured for internal and external BGP peers.

ipv6 bgp neighbor *ipv6_address* **update-source-address** *ipv6_address*

no ipv6 bgp neighbor *ipv6_address* **update-source-address** *ipv6_address*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.

Defaults

By default, the update-source-address value is set to all zeros.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The BGP peer is restarted after issuing this command.
- The default is restored by using the **no** form of the command or by entering an all-zero address.

Examples

```
-> ipv6 bgp neighbor 2001::1 update-source-address 2401::1
-> no ipv6 bgp neighbor 2001::1 update-source-address
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor update-source	Configures the local IPv6 interface from which a BGP peer will be connected.
show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgPeer6LocalAddr
```

ipv6 bgp neighbor passive

Configures the local IPv6 BGP speaker to wait for this IPv6 BGP peer to establish a connection. When enabled, the local BGP speaker will not initiate a peer session with this peer; in this sense, the BGP speaker is “passive.” When disabled, the local BGP speaker will attempt to set up a session with this peer.

ipv6 bgp neighbor *ipv6_address* **passive**

no ipv6 bgp neighbor *ipv6_address* **passive**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable passive peer behavior.
- By default, BGP will initiate a session to a peer once the peer is configured, has an AS number, and is enabled. You can use this command to configure the local BGP speaker as passive and an outbound session will not be initiated to this peer. For such peers, BGP will always wait passively for the inbound session attempt.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::1 passive
-> no ipv6 bgp neighbor 2001::1 passive
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor	Creates or deletes a BGP peer relationship using IPv6 addresses.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6Passive
```

ipv6 bgp neighbor remove-private-as

Enables or disables the stripping of private autonomous system numbers from the AS path of routes destined to this peer.

ipv6 bgp neighbor *ipv6_address* **remove-private-as**

no ipv6 bgp neighbor *ipv6_address* **remove-private-as**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable stripping of private AS numbers.
- By default, all AS numbers in the AS path are passed to peers. Enabling this command strips any private AS numbers in the AS path before sending updates to this peer. AS numbers in the range 64512 to 65535 are considered private ASs; they are intended for internal use within an organization (such as an enterprise network), but they are not intended for use on public networks (such as the Internet).
- This command has no effect if you are not using ASs in the range 64512 to 65535.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::1 remove-private-as
-> no ipv6 bgp neighbor 2001::1 remove-private-as
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor remote-as	Assigns an AS number to the BGP peer.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgPeer6RemovePrivateAs
```

ipv6 bgp neighbor soft-reconfiguration

Enables or disables IPv6 BGP peer soft reconfiguration. Soft reconfiguration increases the stability of the peer by allowing you to reconfigure attributes that require peer resets without halting the TCP connection with other peers.

ipv6 bgp neighbor *ipv6_address* **soft-reconfiguration**

no ipv6 bgp neighbor *ipv6_address* **soft-reconfiguration**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.

Default

This command is enabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- This feature stores routes and other configuration information in local memory. When you make configuration changes that require a peer reset, the routing cache is not cleared and connections with other peers are not interrupted.
- If a peer is not route-refresh capable, by default, BGP stores all paths from peers, even those that are policy rejected, in anticipation of policy changes in the future. Storing these paths consumes memory. You can use this command to disable the storing of these paths, or soft reconfiguration. However, if soft reconfiguration is disabled and the peer is not route-refresh capable and the inbound policy changes, the peer will have to be restarted using the **ipv6 bgp neighbor clear** command.
- If the peer is route-refresh capable and soft reconfiguration is disabled, inbound policy changes are still supported without re-starting the peer.

Examples

```
-> ipv6 bgp neighbor 2001::1 soft-reconfiguration
-> no ipv6 bgp neighbor 2001::1 soft-reconfiguration
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor clear	Restarts the IPv6 BGP peer.
ipv6 bgp neighbor clear soft	Invokes an inbound or outbound policy reconfiguration for an IPv6 BGP peer.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6SoftReconfig
```

ipv6 bgp neighbor stats-clear

Clears the statistics for a peer.

ipv6 bgp neighbor *ipv6_address* **stats-clear**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command clears the statistical variables for a peer so they can accumulate from a known point.
- The cleared statistics include the total messages sent and received from this peer, the total UPDATE messages sent and received from this peer, the total NOTIFY messages sent and received from this peer, and the total peer state transition messages sent and received from this peer. These statistics can be displayed through **show ipv6 bgp neighbors statistics**.

Examples

```
-> ipv6 bgp neighbor 2001::2 stats-clear
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors statistics	Displays the neighbor statistics of the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ClearCounter
```

ip bgp confederation neighbor6

Configures this IPv6 BGP peer as a member of the same confederation as the local BGP speaker.

ip bgp confederation neighbor6 *ipv6_address*

no ip bgp confederation neighbor6 *ipv6_address*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- You must first assign a confederation number to the local BGP speaker before assigning peers to the confederation. Use the **ip bgp confederation identifier** command to assign a confederation number to the local BGP speaker.

Examples

```
-> ip bgp confederation neighbor6 2001::1
-> no ip bgp confederation neighbor6 2001::1
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip bgp confederation identifier	Sets a confederation identification value for the local BGP speaker (this router).

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeerAddr
   alaBgPeer6ConfedStatus
```

ipv6 bgp neighbor in-aspathlist

Assigns an inbound AS path list filter to a BGP peer.

ipv6 bgp neighbor *ipv6_address* **in-aspathlist {***string* | **none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
string	Inbound AS path list (0 to 70 characters). This name is case sensitive.
none	Removes this AS path list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The AS path list name *(***InboundASpath** in the example below) is created using the **ip bgp policy aspath-list** command. Any inbound routes from the BGP peer must match this AS path filter before being accepted or passed to an inbound policy.
- Use **none** to deassign an AS path filter list from this peer.

Examples

```
-> ipv6 bgp neighbor 2001::1 in-aspathlist InBoundASpath
-> ipv6 bgp neighbor 2001::1 in-aspathlist none
```

Release History

Release 7.3.4; command introduced.

Related Commands

ip bgp policy aspath-list	Creates or removes an AS path list.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6AspathListIn
```

ipv6 bgp neighbor in-communitylist

Assigns an inbound community list filter to a BGP peer.

ipv6 bgp neighbor *ipv6_address* **in-communitylist {***string* | **none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
string	Input community list (0 to 70 characters). This name is case sensitive.
none	Removes this community list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The community filter list name (**InboundCommlist** in the example below) is created using the **ip bgp policy community-list** command. Any inbound routes from the BGP peer must match this community filter before being accepted or passed to inbound policy.
- Use **none** to deassign an input community filter list from this peer.

Examples

```
-> ipv6 bgp neighbor 2001::1 in-communitylist InboundCommlist
-> ipv6 bgp neighbor 2001::1 in-communitylist none
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6CommunityListIn
```

ipv6 bgp neighbor in-prefixlist

Assigns an inbound prefix filter list to a BGP peer.

ipv6 bgp neighbor *ipv6_address* **in-prefixlist {***string* | **none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
string	Input prefix filter list (0 to 70 characters). This name is case sensitive.
none	Removes the prefix list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix list name (**InboundPrefix** in the example below) is created using the **ip bgp policy prefix-list** command. Any inbound IPv4 routes from the BGP peer must match this prefix filter before being accepted or passed to inbound policy.
- Use **none** to deassign an input prefix filter list from this peer.

Examples

```
-> ipv6 bgp neighbor 2001::1 in-prefixlist InboundPrefix
-> ipv6 bgp neighbor 2001::1 in-prefixlist none
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6PrefixListIn
```

ipv6 bgp neighbor in-prefix6list

Assigns an inbound prefix6 list to a BGP peer.

ipv6 bgp neighbor *ipv6_address* **in-prefix6list {***string* | **none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
string	Input prefix6 filter list (0 to 70 characters). This name is case sensitive.
none	Removes the prefix6 list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix6 list name (**InboundPrefix6** in the example below) is created using the **ip bgp policy prefix6-list** command. Any inbound IPv6 routes from the BGP peer must match this prefix6 filter before being accepted or passed to inbound policy.
- To deassign an input prefix6 filter list, use this command to assign a value of "**none.**"

Examples

```
-> ipv6 bgp neighbor 2001::2 in-prefix6list InboundPrefix6
-> ipv6 bgp neighbor 2001::2 in-prefix6list none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Prefix6ListIn
```

ipv6 bgp neighbor out-aspathlist

Assigns an outbound AS path filter list to a BGP peer.

ipv6 bgp neighbor *ipv6_address* **out-aspathlist {***string* | **none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
string	Outbound AS path list (0 - 70 characters).
none	Removes the AS path list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The AS path list name (**OutboundASpath** in the example below) is created using the **ip bgp policy aspath-list** command. Any outbound routes from the BGP peer must match this AS path filter, or policy, before being advertised or passed to outbound policy.
- Use **none** to deassign an output AS path filter list from this peer.

Examples

```
-> ipv6 bgp neighbor 2001::1 out-aspathlist OutboundASpath
-> ipv6 bgp neighbor 2001::1 out-aspathlist none
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip bgp policy aspath-list	Creates or removes an AS path list.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6AspathListOut
```

ipv6 bgp neighbor out-communitylist

Assigns an outbound community filter list to a BGP peer.

ipv6 bgp neighbor *ipv6_address* **out-communitylist {***string* **| none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
string	Outbound AS path list (0 - 70 characters).
none	Removes the community list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The community filter list name (**OutboundCommlist** in the example below) is created using the **ip bgp policy community-list** command. Any outbound routes from the BGP peer must match this community filter before being advertised or passed to outbound policy.
- Use **none** to deassign an output community filter list from this peer.

Examples

```
-> ipv6 bgp neighbor 2001::1 out-communitylist OutboundCommlist
-> ipv6 bgp neighbor 2001::1 out-communitylist none
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6CommunityListOut
```

ipv6 bgp neighbor out-prefixlist

Assigns an outbound prefix filter list to a BGP peer.

ipv6 bgp neighbor *ipv6_address* **out-prefixlist {***string* | **none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
string	Outbound prefix filter list (0 - 70 characters).
none	Removes the prefix filter list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix list name (**OutboundPrefix** in the example below) is created using the **ip bgp policy prefix-list** command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to an outbound policy.
- Use **none** to deassign an output prefix filter list from this peer.

Examples

```
-> ipv6 bgp neighbor 2001::1 out-prefixlist OutboundPrefix
-> ipv6 bgp neighbor 2001::1 out-prefixlist none
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6PrefixListOut
```

ipv6 bgp neighbor out-prefix6list

Assigns an outbound prefix6 filter list to a BGP peer.

ipv6 bgp neighbor *ipv6_address* **out-prefix6list {***string* | **none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the BGP peer.
string	Outbound prefix6 filter list (0 - 70 characters).
none	Removes the prefix6 filter list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The prefix6 list name (**OutboundPrefix6** in the example below) is created using the **ip bgp policy prefix6-list** command. Any outbound IPv6 routes from the BGP peer must match this prefix6 filter before being advertised or passed to outbound policy.
- To deassign an output prefix6 filter list, use this command to assign a value of "**none**".

Examples

```
-> ipv6 bgp neighbor 2001::2 out-prefix6list OutboundPrefix6
-> ipv6 bgp neighbor 2001::2 out-prefix6list none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Prefix6ListOut
```

ipv6 bgp neighbor route-map

Assigns a policy map to an IPv6 BGP peer.

ipv6 bgp neighbor *ipv6_address* **route-map {***string* **| none} {in | out}**

no ipv6 bgp neighbor *ipv6_address* **route-map {in | out}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address of the peer.
string	Policy map name (0 to 70 characters). This name is case sensitive.
none	Deletes the route map if entered rather than a text string.
in	Designates this route map policy as an inbound policy.
out	Designates this route map policy as an outbound policy.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no f**orm of this command to deassign a policy map.
- The policy route map name (**InboundRoute** and **OutboundRoute** in the example below) is created using the **ip bgp policy route-map** command. Any routes from the BGP peer must match this route map filter before being accepted or passed to a policy.
- It is also possible to deassign a route map by entering **none** in place of a route map name.

Examples

```
-> ipv6 bgp neighbor 2001::1 route-map InboundRoute in
-> ipv6 bgp neighbor 2001::1 route-map OutboundRoute out
-> ipv6 bgp neighbor 2001::1 route-map none in
-> no ipv6 bgp neighbor 2001::1 route-map in
```

Release History

Release 7.3.4; command introduced.

Related Commands

ip bgp policy route-map	Creates or deletes a policy route map.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6RouteMapIn
   alaBgpPeer6RouteMapOut
```

ipv6 bgp neighbor clear soft

Invokes an inbound or outbound policy reconfiguration for an IPv6 BGP peer.

ipv6 bgp neighbor *ipv6_address* **clear soft {in | out}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.
in	Applies reconfiguration to the inbound policies.
out	Applies reconfiguration to the outbound policies.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command reconfigures (or reapplies) all inbound or outbound policies to existing routes without restarting the peer session.
- This command is useful if policies have been changed.

Examples

```
-> ipv6 bgp neighbor 2001::1 clear soft in
-> ipv6 bgp neighbor 2001::1 clear soft out
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp neighbor soft-reconfiguration	Enables or disables IPv6 BGP peer soft reconfiguration.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6ReconfigureInBound
   alaBgpPeer6ReconfigureOutBound
```

ipv6 bgp neighbor route-reflector-client

Configures this IPv6 BGP peer as one of the clients to the local route reflector.

ipv6 bgp neighbor *ipv6_address* **route-reflector-client**

no ipv6 bgp neighbor *ipv6_address* **route-reflector-client**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.

Defaults

By default, the command is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the no form of this command to disable IPv6 BGP peer as a client to the local route reflector.
- The IPv6 BGP peers configured using this command become part of the client group. The remaining peers become the members of the non-client group for the local route reflector.
- When IPv6 BGP Peer is configured as route reflector client, all internal BGP speakers in an autonomous system need not be fully meshed. Instead, this route reflector takes the responsibility for passing internal BGP-learned routes to its peers.

Examples

```
-> ipv6 bgp neighbor 2001::1 route-reflector-client
-> no ipv6 bgp neighbor 2001::1 route-reflector-client
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show ipv6 bgp neighbors .Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ClientStatus
```

ipv6 bgp neighbor md5 key

Configures an encrypted MD5 signature for TCP sessions with this IPv6 peer.

ipv6 bgp neighbor *ipv6_address* **md5 key {***string* **| none}**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP peer.
string	The MD5 public key. The maximum character length is 80.
none	Remove the password and disable authentication.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The BGP peer is restarted after issuing this command.
- The password you specified in this command is encrypted before it appears in a saved snapshot file. However, if you view this command in a snapshot file or **boot.cfg** file, the command is displayed in a different syntax as given below:

  ipv6 bgp neighbor *ipv6_address* **md5 key-encrypt** *encrypted_string*

Note. This MD5 password will not work, if this syntax is used to set it.

Examples

```
-> ipv6 bgp neighbor 2001::1 md5 key openpeer2
-> ipv6 bgp neighbor 2001::1 md5 key none
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 bgp neighbor	Creates or deletes a BGP peer relationship using IPv6 addresses.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6MD5Key
```

show ipv6 bgp neighbors

Displays the configured IPv6 BGP peers.

show ipv6 bgp neighbors [*ipv6_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address for the BGP neighbor.

Defaults

By default, all the configured IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the *ipv6_address* parameter to display the details of a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors
Legends: Nbr = Neighbor
         As  = Autonomous System
Nbr address              As   Admin state Oper state  BGP Id   Up/Down      BFD
                                                                           Status
-----------------------+----+-----------+-----------+--------+-----------+--------
2001:100:3:4::1          30   enabled     established 11.4.0.1 01h:42m:08s enabled
fe80::200:57ff:fe28:7e89 10   enabled     established 11.5.0.1 01h:40m:58s disabled

-> show ipv6 bgp neighbors 2001:100:3:4::1
Neighbor address                  = 2001:100:3:4::1,
Neighbor autonomous system        = 30,
Neighbor Admin state              = enabled,
Neighbor Oper state               = established,
Neighbor passive status           = disabled,
Neighbor name                     = peer(2101::51),
Neighbor local address            = 2001:100:3:4::10,
Neighbor EBGP multiHop            = disabled,
Neighbor next hop self            = disabled,
Neighbor TTL security             = 6,
Neighbor Route Refresh            = enabled,
Neighbor Ipv4 unicast             = enabled,
Neighbor Ipv4 multicast           = disabled,
Neighbor type                     = internal,
Neighbor auto-restart             = enabled,
Neighbor route-reflector-client   = disabled,
Neighbor confederation status     = disabled,
Neighbor remove private AS        = disabled,
Neighbor default originate        = disabled,
Neighbor maximum prefixes         = 5000,
Neighbor max prefixes warning     = enabled,
```

```
# of prefixes received            = 10,
Neighbor MD5 key                  = <none>,
Neighbor local port               = 49154,
Neighbor TCP window size          = 32768,
Graceful Restart State            = NotRestarting,
Advertised Restart Interval       = 0s,
Forwarding State during restart   = NotPreserved,
Activate IPv6 unicast             = enabled,
Configured IPv4 NextHop Address   = 0.0.0.0,
Configured IPv6 NextHop Address   = ::,
Neighbor Ipv6 unicast             = advertised,
BFD Status                        = enabled
Activate IPv4 unicast             = enabled
```

output definitions

Nbr address or **Neighbor address**	The IPv6 address for this BGP peer. Assign this address through the **ipv6 bgp neighbor** command.
As or **Neighbor autonomous system**	The autonomous system to which this peer belongs. A peer's AS number is assigned through the **ipv6 bgp neighbor remote-as** command.
Admin state or **Neighbor Admin state**	Indicates whether this peer has been enabled or disabled through the **ipv6 bgp neighbor admin-state** command.
Oper state or **Neighbor Oper state**	The current BGP state for this peer. Possible states are **idle**, **connect**, **active**, **opensent**, **openconfirm**, and **established**.
BGP Id	The unique BGP identifier of the peer.
Up/Down	The time since this peer has transitioned to its current UP or DOWN state. If the peer is currently Established, then this is the time that the peer has been UP. If the peer is currently Idle, then this is the time the peer has been DOWN.
Neighbor passive status	Indicates whether the local BGP speaker is "passive" (i.e., waiting for this peer to initiate a session).
Neighbor name	The name assigned to this peer.
Neighbor local address	The interface assigned to this peer. This value is configured through the **ipv6 bgp neighbor update-source** command.
Neighbor EBGP multiHop	Indicates whether BGP multi-hop support is enabled or disabled. This supports allows external BGP peers to communicate with each other even when they are not directly connected.
Neighbor next hop self	Indicates whether this peer is using next hop processing. This value is configured through the **ipv6 bgp neighbor next-hop-self** command.
Neighbor TTL security	Displays the number of hops between the switch and the peer. If the GTSM is disabled the value is displayed as none.
Neighbor Route Refresh	Indicates whether this peer supports Route Refresh capability as defined in RFC 2918. This capability is an alternative to soft-reconfiguration that can save CPU and memory resources. It allows peers to dynamically request the re-advertisement of BGP routing tables. Since this router supports route refresh all BGP peers are automatically enabled for this capability.
Neighbor Ipv4 unicast	Indicates whether this peer is multiprotocol IPv4 unicast capable.

output definitions (continued)

Neighbor Ipv4 multicast	Indicates whether this peer is multiprotocol IPv4 multicast capable.
Neighbor type	Indicates whether this peer is internal or external to the AS.
Neighbor auto-restart	Indicates whether peer auto-restart is enabled or disabled.
Neighbor route-reflector-client	Indicates whether this peer is a client to the local route reflector, if configured.
Neighbor confederation status	Indicates whether this peer is a member of a BGP confederation.
Neighbor remove private AS	Indicates whether the stripping of private AS numbers (64512 to 65535) from AS paths is enabled or disabled.
Neighbor default originate	Indicates whether peer default origination is enabled or disabled. When enabled, the local BGP speaker advertises the default route to the peer. This value is configured through the **ipv6 bgp neighbor default-originate** command.
Neighbor maximum prefixes	The maximum number of prefixes the local router can receive in UPDATE from this peer. This value is configured through the **ipv6 bgp neighbor maximum-prefix** command.
Neighbor max prefixes warning	Indicates whether a warning will be issued when this peer exceeds 80 percent of the maximum prefix value. This value is configured through the **ipv6 bgp neighbor update-source** command.
# of prefixes received	Displays the total number of prefixes received by this neighbor.
Neighbor MD5 key	When present, shows an encrypted version of the MD5 password. When not present, and MD5 password has not been configured.
Neighbor local port	The TCP port used for the session with this peer.
Neighbor TCP window size	The size of the TCP window for this BGP session. This value will always be 32768 as that is the maximum size of a BGP message.
Graceful Restart State	Indicates the graceful restart state. This feature does not support IPv6 prefixes.
Advertised Restart Interval	Indicates the restart interval in seconds.
Forwarding State during restart	Indicates whether the peer has preserved the forwarding state during the graceful restart.
Activate IPv6 unicast	Indicates whether or not IPv6 unicast advertisements are enabled. Options include **enabled** or **disabled**.
Configured IPv4 NextHop Address	Specifies the IPv4 nexthop address. This is specified using the **ipv6 bgp neighbor ipv4-nexthop** command.
Configured IPv6 NextHop Address	Specifies the IPv6 nexthop address. This is specified using the **ipv6 bgp neighbor ipv6-nexthop** command.
Neighbor Ipv6 unicast	Indicates whether or not IPv6 unicast capability is advertised between the peers. Options include **enabled** or **disabled**.
BFD Status	Indicates whether BFD is enabled or disabled for this peer. The BFD status is configured through the **ip|ipv6 bgp neighbor bfd-state** command.
Activate IPv4 unicast	Indicates whether or not IPv4 unicast capability is advertised between the peers. Options include **enabled** or **disabled**.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; ‘Activate IPv4 unicast’ output field added.
Release 8.4.1; ‘Neighbor TTL security’ output field added.

Related Commands

ipv6 bgp neighbor	Creates or deletes a BGP peer relationship using IPv6 addresses
ipv6 bgp neighbor admin-state	Enables or disables the BGP peer status.
ipv6 bgp neighbor ttl-security	Configures the Generalized TTL Security Mechanism (GTSM) for the BGP peer.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6AS
   alaBgpPeer6Passive
   alaBgpPeer6Name
   alaBgpPeer6MultiHop
   alaBgpPeer6MaxPrefix
   alaBgpPeer6MaxPrefixWarnOnly
   alaBgpPeer6NextHopSelf
   alaBgpPeer6TTLSecurityHops
   alaBgpPeer6SoftReconfig
   alaBgpPeer6InSoftReset
   alaBgpPeer6Ipv4Unicast
   alaBgpPeer6Ipv4Multicast
   alaBgpPeer6RcvdRtRefreshMsgs
   alaBgpPeer6SentRtRefreshMsgs
   alaBgpPeer6RouteMapOut
   alaBgpPeer6RouteMapIn
   alaBgpPeer6LocalAddr
   alaBgpPeer6LastDownReason
   alaBgpPeer6LastDownTime
   alaBgpPeer6LastReadTime
   alaBgpPeer6RcvdNotifyMsgs
   alaBgpPeer6SentNotifyMsgs
   alaBgpPeer6LastSentNotifyReason
   alaBgpPeer6LastRecvNotifyReason
   alaBgpPeer6RcvdPrefixes
   alaBgpPeer6DownTransitions
   alaBgpPeer6Type
   alaBgpPeer6AutoReStart
   alaBgpPeer6ClientStatus
   alaBgpPeer6ConfedStatus
   alaBgpPeer6RemovePrivateAs
   alaBgpPeer6ClearCounter
   alaBgpPeer6TTL
   alaBgpPeer6AspathListOut
   alaBgpPeer6AspathListIn
   alaBgpPeer6PrefixListOut
   alaBgpPeer6PrefixListIn
   alaBgpPeer6CommunityListOut
   alaBgpPeer6CommunityListIn
   alaBgpPeer6Restart
   alaBgpPeer6DefaultOriginate
   alaBgpPeer6ReconfigureInBound
   alaBgpPeer6ReconfigureOutBound
   alaBgpPeer6MD5Key
   alaBgpPeer6MD5KeyEncrypt
   alaBgpPeer6RowStatus
   alaBgpPeer6UpTransitions
   alaBgpPeer6LastWriteTime
   alaBgpPeer6AdminStatus
   alaBgpPeer6State
   alaBgpPeer6LocalPort
   alaBgpPeer6TcpWindowSize
   alaBgpPeer6ActivateIpv6
   alaBgpPeer6ActivateIpv4
```

show ipv6 bgp neighbors statistics

Displays the neighbor statistics of the configured IPv6 BGP peers.

show ipv6 bgp neighbors statistics [*ipv6_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.

Defaults

By default, the neighbor statistics for all the IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the *ipv6_address* parameter to display the neighbor statistics of a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors statistics
Legends: Nbr   = Neighbor
         As    = Autonomous System
         RMSGS = # of received messages
         SMSGS = # of sent messages
         RUPDS = # of Update messages received
         SUPDS = # of Update messages sent
         RNOFY = # of Notify messages received
         SNOFY = # of Notify messages sent
         RPFXS = # of prefixes received
         UPTNS = # of UP transitions
         DNTNS = # of DOWN transitions

Nbr address             As    RMSGS SMSGS RUPDS SUPDS RNOFY SNOFY RPFXS UPTNS DNTNS
------------------------+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
2001:100:3:4::1         30    225   260   2     3     0     0     10    1     1
```

output definitions

Nbr address	The IPv6 address for this peer. This value is configured using the **ipv6 bgp neighbor** command.
As	The autonomous system to which this peer belongs. This value is configured using the **ipv6 bgp neighbor remote-as** command.
RMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.
SMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent by this peer.

output definitions (continued)

RUPDS	The number of route UPDATE messages received by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
SUPDS	The number of route UPDATE messages sent by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
RNOFY	The number of NOTIFY messages received by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
SNOFY	The number of NOTIFY messages sent by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
RPFXS	Number of unique route prefixes received by this peer.
UPTNS	Number of times this peer has come up, operationally.
DNTNS	Number of times this peer has gone down, operationally.

```
-> show ipv6 bgp neighbors statistics 2001:100:3:4::1
Neighbor address                  = 2001:100:3:4::1,
# of UP transitions               = 1,
Time of last UP transition        = 01h:50m:36s,
# of DOWN transitions             = 1,
Time of last DOWN transition      = 00h:00m:00s,
Last DOWN reason                  = none,
# of msgs rcvd                    = 226,
# of Update msgs rcvd             = 2,
# of prefixes rcvd                = 10,
# of Route Refresh msgs rcvd      = 0,
# of Notification msgs rcvd       = 0,
Last rcvd Notification reason     = none [none]
Time last msg was rcvd            = 00h:00m:04s,
# of msgs sent                    = 260,
# of Update msgs sent             = 3,
# of Route Refresh msgs sent      = 0
# of Notification msgs sent       = 0,
Last sent Notification reason     = none [none]
Time last msg was sent            = 00h:00m:18s,
```

output definitions

Neighbor address	The IPv6 address for this peer. This value is configured using the **ipv6 bgp neighbor** command.
# of UP transitions	Number of times this peer has come up, operationally.
Time of last UP transition	The duration that this peer has been up.
# of DOWN transitions	Number of times this peer has gone down, operationally.
Time of last DOWN transition	The duration since this peer last went down.

output definitions (continued)

Last DOWN reason	Provides a message as the last reason why a peer went down. The possible reasons for going down are: user_request - user initiated conn_timeout - connection timer expired hold_timeout - hold timer expired bad_msg - received a bad message from neighbor fsm_blink - BGP FSM error peer_closed - neighbor closed connection peer_notify - neighbor sent fatal notification tcp_error - Fatal TCP error none - None
# of msgs rcvd	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.
# of Update msgs rcvd	The number of route UPDATE messages received from this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# **of prefixes rcvd**	Number of unique route prefixes received by this peer.
# of Route Refresh msgs rcvd	Number of route refresh requests this peer has received. Route refresh requests all routes learned be a peer.
# **of Notification msgs rcvd**	Number of NOTIFY messages received from this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last rcvd Notification reason	NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message received from this peer. The notification reasons are listed in two parts separated by a dash (-). The following are possible notification reasons: message header error - synchronization loss message header error - bad length message header error - bad type open message error - unsupported version open message error - bad peer autonomous system open message error - bad peer bgp id open message error - unsupported option open message error - authentication failure open message error - unacceptable hold time open message error - unsupported capability update message error - malformed attribute update message error - unknown attribute update message error - missing wellknown attribute update message error - attribute flags error update message error - attribute length error update message error - invalid origin update message error - as loop update message error - invalid nexthop update message error - optional attribute error update message error - invalid network update message error - malformed aspath cease - maximum number of prefixes reached cease - administrative shutdown cease - peer de-configured cease- administrative reset cease- connection rejected cease - other configuration change cease - connection collision resolution cease - out of resources hold time out - none fsm error - none none - none
Time last msg was rcvd	The duration since a message was received from this peer.
# of msgs sent	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent to this peer.
# of Update msgs sent	Number of route UPDATE messages sent to this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of Route Refresh msgs sent	Number of route refresh requests this peer has sent. Route refresh requests request all routes learned be a peer.
# of Notification msgs sent	Number of NOTIFY messages sent to this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last sent Notification reason	NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message sent by this peer. The notification reasons are listed in two parts separated by a dash (-). See the list of possible notification reasons under the description for the **Peer last received notification reason** field above.
Time last msg was sent	The duration since a message was sent to this peer.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6RcvdMsgs
   alaBgpPeer6SentMsgs
   alaBgpPeer6RcvdUpdMsgs
   alaBgpPeer6SentUpdMsgs
   alaBgpPeer6LastTransitionTime
   alaBgpPeer6LastUpTime
   alaBgpPeer6BgpId
   alaBgpPeer6LocalIntfName
   alaBgpPeer6RestartTime
   alaBgpPeer6RestartState
   alaBgpPeer6RestartFwdState
   alaBgpPeer6Ipv6Unicast
   alaBgpPeer6HoldTime
   alaBgpPeer6KeepAlive
   alaBgpPeer6ConnRetryInterval
   alaBgpPeer6HoldTimeConfigured
   alaBgpPeer6KeepAliveConfigured
   alaBgpPeer6Ipv4NextHop
   alaBgpPeer6Ipv6NextHop
```

show ipv6 bgp neighbors policy

Displays the incoming and outgoing prefix6 list policy identifiers configured for BGP IPv6 peer.

show ipv6 bgp neighbors policy *ipv6_address*

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command displays all of the configured policies for the router, or the polices configured for a specific BGP IPv6 peer.

Examples

```
-> show ipv6 bgp neighbors policy
Neighbor address  =  2001::1,
  Neighbor autonomous system          = 1,
  Neighbor output policy map name     = <none>,
  Neighbor input policy map name      = <none>,
  Neighbor output aspath-list name    = <none>,
  Neighbor input aspath-list name     = <none>,
  Neighbor output prefix-list name    = <none>,
  Neighbor input prefix-list name     = <none>,
  Neighbor output community-list name = <none>,
  Neighbor input community-list name  = <none>,
  Neighbor soft reconfiguration       = enabled
  Neighbor output prefix6-list name   = <none>,
  Neighbor input prefix6-list name    = <none>
```

output definitions

Neighbor autonomous system	The AS to which the peer is assigned. This can be assigned by using the **ipv6 bgp neighbor remote-as** command.
Neighbor output policy map name	The outbound route map policy for the peer. This can be assigned by using the **ipv6 bgp neighbor route-map** command.
Neighbor input policy map name	The inbound route map policy for the peer. This can be assigned by using the **ipv6 bgp neighbor route-map** command.
Neighbor output aspath-list name	The outbound AS path list policy for the peer. This can be assigned by using the **ipv6 bgp neighbor out-aspathlist** command.

output definitions (continued)

Neighbor input aspath-list name	The inbound AS path list policy for the peer. This can be assigned by using the **ipv6 bgp neighbor in-aspathlist** command.
Neighbor output prefix-list name	The outbound prefix list policy for the peer. This can be assigned by using the **ipv6 bgp neighbor out-prefixlist** command.
Neighbor input prefix-list name	The inbound prefix list policy for the peer. This can be assigned by using the **ipv6 bgp neighbor in-prefixlist** command.
Neighbor output community-list name	The outbound community list policy for the peer. This can be assigned by using the **ipv6 bgp neighbor out-communitylist** command.
Neighbor input community-list name	The inbound community list policy for the peer. This can be assigned by using the **ipv6 bgp neighbor in-communitylist** command.
Neighbor soft reconfiguration	Lists whether soft reconfigurations are enabled or disabled for this peer. This is configured using the **ipv6 bgp neighbor soft-reconfiguration** command.
Neighbor output prefix6-list name	The outbound prefix6-list policy for the peer. This is configured using the **ipv6 bgp neighbor out-prefix6list** command.
Neighbor input prefix6-list name	The inbound prefix6-list policy for the peer. This is configured using the **ipv6 bgp neighbor in-prefix6list** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays configured IPv6 BGP peers

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6AS
   alaBgpPeer6RouteMapOut
   alaBgpPeer6RouteMapIn
   alaBgpPeer6AspathListOut
   alaBgpPeer6AspathListIn
   alaBgpPeer6PrefixListOut
   alaBgpPeer6PrefixListIn
   alaBgpPeer6CommunityListOut
   alaBgpPeer6CommunityListIn
   alaBgpPeer6SoftReconfig
   alaBgpPeer6Prefix6ListOut
   alaBgpPeer6Prefix6ListIn
```

show ipv6 bgp neighbors timers

Displays the timers for configured IPv6 BGP peers.

show ipv6 bgp neighbors timers [*ipv6_address***]**

Syntax Definitions

ipv6_address	The 128-bit IPv6 address.

Defaults

By default, the timer values for all the IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the *ipv6_address* parameter to display the timer value for a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors timers
Legends: Nbr     = Neighbor
         As      = Autonomous System
         RtAdv   = Route Advertisement
         Kalive  = Keep Alive (actual)
         Ka(C)   = Configured Keep Alive
Nbr address                        As    Hold  Hold(C) RtAdv Retry Kalive Ka(C)
-----------------------------------+-----+-----+-------+-----+-----+------+-----
2001:100:3:4::1                     30    90    90      30    120   30     30
```

output definitions

Nbr address	The IPv6 address for this BGP peer. Assign this address using the **ipv6 bgp neighbor** command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned using the **ipv6 bgp neighbor remote-as** command.
Hold	The actual negotiated hold time value.
Hold (C)	The hold time value. This value is configured using the **ipv6 bgp neighbor timers** command.
RtAdv	The route advertisement interval, in seconds, for updates between external BGP peers.
Retry	The interval, in seconds, between retries by this peer to set up a connection through TCP with another peer. This value is configured using the **ipv6 bgp neighbor timers** command.

output definitions (continued)

Kalive	The actual negotiated value, in seconds, between KEEPALIVE messages. KEEPALIVE messages do not contain route or status updates; they serve only to tell other peers that the connection is still live and this peer is reachable.
Ka (C)	The KEEPALIVE interval as configured using the **ipv6 bgp neighbor timers** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp statistics	Displays BGP global statistics.

MIB Objects

```
alaBgpPeer6Table
   alaBgpPeer6Addr
   alaBgpPeer6ConnRetryInterval
   alaBgpPeer6MinRouteAdvertisementInterval
   alaBgpPeer6HoldTime
```

30 Server Load Balancing Commands

Server Load Balancing (SLB) allows clients to send requests to servers logically grouped together in clusters. Each cluster logically aggregates a set of servers running identical applications with access to the same content (for example, web servers). Clients access clusters through the use of a Virtual IP (VIP) address.

MIB information for the SLB commands is as follows:

Filename ALCATEL-IND1-SLB-MIB.mib
Module: alcatelIND1SLBMIB

A summary of available commands is listed here:

Global SLB Commands	**ip slb admin-state** **ip slb reset statistics** **show ip slb**
SLB Cluster Commands	**ip slb cluster** **ip slb cluster admin-state** **ip slb cluster ping period** **ip slb cluster ping timeout** **ip slb cluster ping retries** **ip slb cluster probe** **show ip slb clusters** **show ip slb cluster**
SLB Server Commands	**ip slb server ip cluster** **ip slb server ip cluster probe** **show ip slb cluster server** **show ip slb servers**
SLB Probe Commands	**ip slb probe** **ip slb probe timeout** **ip slb probe period** **ip slb probe port** **ip slb probe retries** **ip slb probe username** **ip slb probe password** **ip slb probe url** **ip slb probe status** **ip slb probe send** **ip slb probe expect** **show ip slb probes**

ip slb admin-state

Enables or disables the administrative status for Server Load Balancing (SLB) on a switch.

ip slb admin-state {enable | disable}

Syntax Definitions

enable	Enables the administrative status for Server Load Balancing on a switch.
disable	Disables the administrative status for Server Load Balancing on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Disabling the administrative status for the SLB feature does not delete the SLB configuration from the switch. The next time the feature is enabled, the existing configuration becomes active.

Examples

```
-> ip slb admin-state enable
-> ip slb admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb	Displays the status of Server Load Balancing on a switch.
ip slb cluster	Configures a Server Load Balancing cluster on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbFeatureGroup
   slbAdminStatus
```

ip slb reset statistics

Resets SLB statistics for all clusters configured on the switch.

ip slb reset statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Note that the **qos apply** command resets both QoS statistics *and* SLB cluster statistics. The **ip slb reset statistics** command only resets SLB statistics.

Examples

```
-> ip slb reset statistics
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.

MIB Objects

```
slbFeatureGroup
   slbResetStatistics
```

ip slb cluster

Configures a Server Load Balancing (SLB) cluster on a switch.

ip slb cluster *name* **{vip** *ip_address* **| condition** *string***} [l3 | l2]**

no ip slb cluster *name*

Syntax Definitions

name	The name of the Server Load Balancing (SLB) cluster. The name can consist a maximum of 23 characters. Names with spaces must be enclosed within quotation marks (for example, “mail server”).
ip_address	The Virtual IP (VIP) address for the Server Load Balancing cluster. This IP address must be in dotted decimal format.
string	The name of an existing QoS policy condition that identifies the Server Load Balancing cluster.
l3	Specifies Layer 3 Server Load Balancing mode. The source and destination MAC and TTL of each packet is modified before the packet is bridged or routed to the server.
l2	Specifies Layer 2 Server Load Balancing mode. Packets are not modified before they are bridged to the server. This parameter is only available when using the **condition** parameter.

Defaults

parameter	default
l3 | l2	**l3**

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to delete a Server Load Balancing cluster.
- Once a cluster is created, the Virtual IP or condition cannot be modified. To modify these values, delete the cluster and re-create the cluster with the different VIP and conditions.
- The VIP address of the SLB cluster *must* be an address that is in the same subnet as the servers. In addition, do not specify a VIP address that is already in use by an MCLAG VIP interface. The SLB VIP and MCLAG VIP both provide a common IP address but for different entities and should not share the same IP address.
- Specifying the **l3** parameter when configuring a VIP cluster is not required. VIP clusters only use the Layer-3 mode to route traffic to the servers. Layer-2 mode is not supported with this type of cluster.
- The QoS policy condition must exist before it is assigned to an SLB cluster. Use the **policy condition** command to create the QoS policy condition. See the “QoS Policy Commands” chapter for more information.

- SLB clusters are not active if the Server Load Balancing feature is disabled for the switch. Use the **ip slb admin-state** command to enable this feature.

Note. It is possible to configure clusters and add or remove servers from a cluster even when SLB is disabled for the switch.

Examples

```
-> ip slb cluster corporate_servers vip 1.2.3.4
-> ip slb cluster "mail servers" vip 1.2.3.6
-> ip slb cluster cluster_1 condition intranet_cond l2
-> ip slb cluster cluster_2 condition slb_cond l3
-> no ip slb cluster hr_servers
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb admin-state	Enables or disables Server Load Balancing on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbClusterTable
   slbClusterName
   slbClusterVIP
   slbClusterRowStatus
   slbClusterPackets
   slbClusterCondition
   slbClusterType
```

ip slb cluster admin-state

Administratively enables or disables a Server Load Balancing (SLB) cluster on a switch.

ip slb cluster *cluster_name* **admin-state {enable | disable}**

Syntax Definitions

cluster_name	The name of an existing Server Load Balancing cluster.
enable	Administratively enables a Server Load Balancing cluster on a switch.
disable	Administratively disables a Server Load Balancing cluster on a switch.

Defaults

By default, a cluster is administratively enabled when the cluster is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The SLB cluster name specified with this command must already exist in the switch configuration.

Examples

```
-> ip slb cluster hr_servers admin-state enable
-> ip slb cluster "mail servers" admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster	Configures Server Load Balancing clusters.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbClusterTable
   slbClusterAdminStatus
```

ip slb cluster ping period

Modifies the number of seconds to check the health of the servers in a Server Load Balancing (SLB) cluster.

ip slb cluster *cluster_name* **ping period** *seconds*

Syntax Definitions

cluster_name	The name of the Server Load Balancing cluster.
seconds	The number of seconds for the ping period. Specifying 0 (zero) disables the ping.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

If you do not set the ping period to zero, then the ping period *must* be greater than or equal to the ping timeout value divided by 1000. Use the **ip slb cluster ping timeout** command to modify the ping timeout value.

Examples

```
-> ip slb cluster hr_servers ping period 120
-> ip slb cluster "mail servers" ping period 0
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster ping timeout	Modifies the ping timeout value.
ip slb cluster ping retries	Modifies the number of ping retries.

MIB Objects

```
slbClusterTable
   slbClusterPingPeriod
```

ip slb cluster ping timeout

Configures the ping timeout value for a Server Load Balancing (SLB) cluster before it retries.

ip slb cluster *cluster_name* **ping timeout** *milliseconds*

Syntax Definitions

cluster_name	The name of the Server Load Balancing cluster.
milliseconds	The number of milliseconds for the ping timeout. The valid range for the ping timeout value is 0 to 1000 times the ping period. For example, if the ping period is 10 seconds, then maximum value for the ping timeout is 10000.

Defaults

parameter	default
milliseconds	3000

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **ip slb cluster ping period** command to modify the ping period value.

Examples

```
-> ip slb cluster "mail servers" ping timeout 1000
-> ip slb cluster hr_servers ping timeout 6000
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster ping period	Modifies the ping period value.
ip slb cluster ping retries	Modifies the number of ping retries.

MIB Objects

```
slbClusterTable
   slbClusterPingTimeout
```

ip slb cluster ping retries

Configures the number of ping attempts for a Server Load Balancing (SLB) cluster.

ip slb cluster *cluster_name* **ping retries** *count*

Syntax Definitions

cluster_name	The name of the Server Load Balancing cluster.
count	The number of ping retries.

Defaults

parameter	default
count	3

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb cluster "mail servers" ping retries 5
-> ip slb cluster hr_servers ping retries 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster ping period	Modifies the ping period value.
ip slb cluster ping timeout	Modifies the ping timeout value.

MIB Objects

```
slbClusterTable
   slbClusterPingRetries
```

ip slb cluster probe

Configures a probe for a Server Load Balancing (SLB) cluster.

ip slb cluster *cluster_name* **probe** *probe_name*

Syntax Definitions

cluster_name	The name of the Server Load Balancing cluster.
probe_name	The name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

You must create the probe with the **ip slb probe** before you can use this command.

Examples

```
-> ip slb cluster mail_servers probe mail_server_probe
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
ip slb probe	Configures and deletes SLB probes.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbClusterTable
   slbClusterProbeName
```

ip slb server ip cluster

Adds a physical server to a Server Load Balancing (SLB) cluster, deletes a physical server from an SLB cluster, or modifies the administrative status of a physical server in an SLB cluster.

ip slb server ip *ip_address* **cluster** *cluster_name* **[admin-state {enable | disable}] [weight** *weight***]**

no ip slb server ip *ip_address* **cluster** *cluster_name*

Syntax Definitions

ip_address	The IP address for the physical server.
cluster_name	The name of an existing Server Load Balancing cluster.
enable	Enables a server.
disable	Disables a server.
weight	Specifies the weight of the server.

Defaults

parameter	default
enable | disable	**enable**
weight	**1**

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a physical server from a Server Load Balancing cluster.
- Use the weight parameter to assign the server preference value. Each server or server cluster can be assigned a weight to set their preference value for distribution of incoming network traffic. The weights assigned are relative. For example, if Servers A and B have respective weights of 10 and 20 within a cluster, Server A would get half the traffic of Server B.
- Assigning a weight of 0 (zero) to a server prevents the server from being assigned any new connections. This server is a backup server.
- A higher weight value indicates that the server can accept more network traffic.

Examples

```
-> ip slb server ip 10.255.11.127 cluster corporate_servers
-> ip slb server ip 10.255.11.109 cluster "mail servers" admin-state enable
weight 5
-> no ip slb server ip 10.255.11.105 cluster hr_servers
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb admin-state	Enables or disables Server Load Balancing on a switch.
ip slb cluster	Configures Server Load Balancing clusters.

MIB Objects

```
slbServerTable
   slbServerRowStatus
   slbServerAdminStatus
   slbServerAdminWeight
```

ip slb server ip cluster probe

Configures a probe for a Server Load Balancing (SLB) server.

ip slb server ip *ip_address* **cluster** *cluster_name* **probe** *probe_name*

Syntax Definitions

ip_address	The IP address for the physical server.
cluster_name	The name of the Server Load Balancing cluster.
probe_name	The name of the Server Load Balancing probe.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

You must create the probe with the **ip slb probe** before you can use this command.

Examples

```
-> ip slb server ip 10.255.11.127 cluster corporate_servers probe p_http
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb probe	Configures and deletes SLB probes.
ip slb admin-state	Enables or disables Server Load Balancing on a switch.
ip slb cluster	Configures Server Load Balancing clusters.

MIB Objects

```
slbServerTable
   slbServerProbeName
```

ip slb probe

Configures a Server Load Balancing (SLB) probe used to check the health of servers or clusters.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}**

no ip slb probe *probe_name*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **no** form of this command to delete an SLB probe.

Examples

```
-> ip slb probe mail_server_probe smtp
-> no ip slb probe mail_server_probe
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
```

ip slb probe timeout

Configures the amount of time to wait for Server Load Balancing (SLB) probe answers.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} timeout** *seconds*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
seconds	Specifies the timeout in seconds.

Defaults

parameter	default
seconds	3000

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb probe mail_server smtp timeout 12000
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeTimeout
```

ip slb probe period

Configures the length of time between each SLB probe to check the health of the servers.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} period** *seconds*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
seconds	Specifies the length of time for the SLB probe period.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http period 120
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePeriod
```

ip slb probe port

Configures the TCP/UDP port on which the Server Load Balancing (SLB) probe is sent.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} port** *port_number*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
port_number	Specifies the TDP/UDP port number.

Defaults

parameter	default
port_number	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb probe mis_server udp port 200
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePort
```

ip slb probe retries

Configures the number of Server Load Balancing (SLB) probe retries that are performed before deciding that a server is out of service.

ip slb probe *probe_name* **{ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} retries** *retries*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
retries	Specifies the number of retries.

Defaults

parameter	default
retries	3

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb probe mail_server smtp retries 5
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeRetries
```

ip slb probe username

Configures a user name that is sent to a server as credentials for an HTTP GET operation to verify the health of the server.

ip slb probe *probe_name* **{http | https} username** *user_name*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
user_name	Specifies user name.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http username subnet1
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeHttpUsername
```

ip slb probe password

Configures a password that is sent to a server as credentials for an HTTP GET to verify the health of the server.

ip slb probe *probe_name* **{http | https} password** *password*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
password	Specifies the password.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The password is encrypted in the configuration file so that it is not readable.

Examples

```
-> ip slb probe web_server http password h1f45xc
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeHttpPassword
```

ip slb probe url

Configures a URL that is sent to a server for an HTTP GET to verify the health of the server.

ip slb probe *probe_name* **{http | https} url** *url*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
url	Specifies the URL of the server.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http url pub/index.html
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeHttpUrl
```

ip slb probe status

Configures the expected status returned from an HTTP GET to verify the health of a server.

ip slb probe *probe_name* **{http | https} status** *status_value*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
status_value	Specifies the expected status returned.

Defaults

parameter	default
status_value	200

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http status 404
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePeriod
   slbProbeHttpStatus
```

ip slb probe send

Configures an ASCII string that is sent to a server to invoke a server response and verify the health of the server.

ip slb probe *probe_name* **{tcp | udp} send** *send_string*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
send_string	Specifies the ASCII string sent to a server to invoke a response.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

NA

Examples

```
-> ip slb probe web_server tcp send test
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeSend
```

ip slb probe expect

Configures an ASCII string used to compare a response from a server to verify the health of the server.

ip slb probe *probe_name* **{http | https | tcp | udp} expect** *expect_string*

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
expect_string	Specifies the ASCII string used to compare a response from a server.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http expect test
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbeExpect
```

show ip slb

Displays the status of Server Load Balancing on a switch.

show ip slb

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ip slb

Admin status                    : Enabled,
Operational status              : In Service,
Number of clusters              = 3
```

Output fields are described here:

output definitions

Admin status	The current administrative status of Server Load Balancing (SLB) on this switch (**Enabled** or **Disabled**).
Operational status	The current operational status of Server Load Balancing (SLB) on this switch, which is either **In service** (at least one SLB cluster is in service) or **Out of service** (all SLB clusters are out of service).
Number of clusters	The total number of Server Load Balancing (SLB) clusters on this switch.

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.

MIB Objects

```
slbFeature
   slbAdminStatus
   slbOperStatus
   slbClustersCount
```

show ip slb clusters

Displays the status and basic configuration for all Server Load Balancing (SLB) clusters on a switch. This command also displays traffic statistics for QoS policy condition clusters.

show ip slb clusters [statistics]

Syntax Definitions

statistics	Displays SLB statistics for QoS policy condition clusters.

Defaults

By default, the status and basic configuration for all clusters is displayed; statistics are not shown.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **statistics** parameter to display the total number of packets that were passed to clusters because they met the QoS condition criteria configured for that cluster. The polling interval used to obtain such statistics is every 15 minutes. See the second example below.

Examples

```
-> show ip slb clusters
                                Admin    Operational         #     %
Cluster Name     VIP/COND       Status   Status              Srv   Avail
-----------------+--------------+--------+-------------------+-----+---------
WorldWideWeb     128.241.130.204  Enabled  In Service          3     95
Intranet         128.241.130.205  Enabled  In Service          2     100
FileTransfer     128.241.130.206  Enabled  Out of Service      2     50
```

Output fields are described here:

output definitions

Cluster Name	The name of the SLB cluster.
VIP/COND	The virtual IP (VIP) address or the policy condition name for the SLB cluster.
Admin Status	The administrative status of the SLB cluster (**Enabled** or **Disabled**).
Operational Status	The operational status of the SLB cluster; **In Service** (at least one physical server is operational in the cluster) or **Out of Service**.
# Srv	The total number of physical servers that belong to the SLB cluster.
% Avail	The percentage of time that the physical server has been available for processing client requests. In other words, the actual ratio of up time (**In Service** plus **Retrying**) versus down time (**No Answer** plus **Link Down**). Please note that the **Disabled** and the initial **Discovery** states are not counted as down time.

```
-> show ip slb clusters statistics

                         Admin    Operational
Cluster Name             Status   Status               Count
-----------------------+--------+--------------------+--------
Cluster1                Enabled  In Service           4 Servers
Cluster2                Enabled  In Service           4 Servers

Dst IP 101.113.113.1/255.255.255.255             4503911
Src IP 202.202.1.0/255.255.255.0                 6527831
Src Port 2/49
```

output definitions

Cluster Name	The name of the SLB cluster. This field also contains the administrative and operational status for the cluster and either the VIP address or QoS policy condition value that identifies the cluster.
Admin Status	The administrative state of this physical server (**Enabled** or **Disabled)**.
Operational Status	The operational state of this server. The possible states are described as follows: • **Disabled** (this server is administratively disabled). • **No Answer** (this server has not responded to ping requests). • **Link Down** (there is a bad connection to this server). • **In Service** (this server is used for SLB cluster client connections). • **Discovery** (the SLB cluster is pinging this physical server). • **Retrying** (the SLB cluster is making another attempt to bring up this server).
Count	The total number of physical servers that belong to the cluster, and the total number of packets serviced by the cluster.
Dst	The destination Virtual IP address assigned to the cluster.
Src	Source IP address assigned to the cluster.
Src Port	Source slot and port number of the SLB cluster.

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb reset statistics	Resets SLB statistics for all clusters.
show ip slb cluster	Displays detailed status and configuration information for a single SLB cluster.
show ip slb servers	Displays the status of all physical servers belonging to each SLB cluster on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in an SLB cluster.

MIB Objects

```
slbClusterTable
   slbClusterName
   slbClusterVIP
   slbClusterCondition
   slbClusterAdminStatus
   slbClusterOperStatus
   slbClusterNumberOfServers
   slbClusterNewFlows
slbStatsTable
   slbStatsClusterName
   slbStatsIndex
   slbStatsCounter
slbStatsQualTable
   slbStatsQualType
   slbStatsQualData
```

show ip slb cluster

Displays detailed statistics and configuration information and operational status for a single Server Load Balancing (SLB) cluster. This command also displays traffic statistics for single QoS policy condition cluster.

show ip slb cluster *name* **[statistics]**

Syntax Definitions

name	Specifies the name of the SLB cluster.
statistics	Displays SLB statistics for the specified cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **statistics** parameter to display the total number of packets that were passed to the cluster because they met the QoS condition criteria configured for that cluster. The polling interval used to obtain such statistics is every 15 minutes. See the second example below:

Examples

```
-> show ip slb cluster Intranet

Cluster Intranet
  VIP                           : 128.241.130.204,
  Type                          : L3
  Admin status                  : Enabled,
  Operational status            : In Service,
  Ping period (seconds)         = 60,
  Ping timeout (milliseconds)   = 3000,
  Ping retries                  = 3,
  Probe                         = None,
  Number of packets             = 25346,
  Number of servers             = 3
    Server 128.241.130.107
      Admin status = Enabled, Operational status = In Service,
      Weight = 4, Availability (%) =   0
    Server 128.241.130.117
      Admin status = Enabled, Operational status = Discovery,
      Weight = 6, Availability (%) =   0
    Server 128.241.130.127
      Admin status = Enabled, Operational status = Discovery,
      Weight = 1, Availability (%) =   0
```

output definitions

Cluster	The name of this Server Load Balancing (SLB) cluster.
VIP	The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.
Type	The classifier for the hypothetical packet, which can be **L2** or **L3**.
Admin status	The current administrative status of this Server Load Balancing (SLB) cluster (**Enabled** or **Disabled**).
Operational status	The current operational status of this Server Load Balancing (SLB) cluster, which is **In Service** (at least one physical server is operational in the cluster) or **Out of Service**.
Ping period (seconds)	The ping period (in seconds) used by this Server Load Balancing (SLB) cluster to check the health of physical servers.
Ping timeout (milliseconds)	The timeout (in milliseconds) used by this Server Load Balancing (SLB) cluster to wait for ping answers from physical servers.
Ping retries	The number of ping retries that this Server Load Balancing (SLB) cluster executes before switching the status to **No answer**.
Probe	The probe configured for this cluster.
Number of packets	The number of packets balanced for this Server Load Balancing (SLB) cluster.
Number of servers	The total number of physical servers that belong to this Server Load Balancing (SLB) cluster.
Server	The IP address for this physical server.
Admin Status	The administrative state of this physical server (**Enabled** or **Disabled)**.
Operational Status	The operational state of this server. The possible states are described as follows: • **Disabled** (this server is administratively disabled). • **No Answer** (this server has not responded to ping requests). • **Link Down** (there is a bad connection to this server). • **In Service** (this server is used for SLB cluster client connections). • **Discovery** (the SLB cluster is pinging this physical server). • **Retrying** (the SLB cluster is making another attempt to bring up this server).
Availability (%)	The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (**In Service** plus **Retrying**) versus down time (**No Answer** plus **Link Down**). Please note that the **Disabled** and the initial **Discovery** states are not counted as down time.

```
-> show ip slb cluster Intranet statistics

                         Admin    Operational
Cluster Name             Status   Status               Count
-----------------------+--------+--------------------+--------
Intranet                 Enabled   In Service          3 Servers
Src IP 15.2.3.2/255.255.255.255                       195
       Src Port 1/4
```

output definitions

Cluster Name	The name of the SLB cluster. This field also contains the administrative and operational status for the cluster and either the VIP address or QoS policy condition value that identifies the cluster.
Admin status	The current administrative status of this physical server (**Enabled** or **Disabled**).
Oper status	The operational state of this server. The possible states are described as follows: • **Disabled** (this server is administratively disabled). • **No Answer** (this server has not responded to ping requests). • **Link Down** (there is a bad connection to this server). • **In Service** (this server is used for SLB cluster client connections). • **Discovery** (the SLB cluster is pinging this physical server). • **Retrying** (the SLB cluster is making another attempt to bring up this server).
Count	The total number of physical servers that belong to the cluster, and the total number of packets serviced by the cluster.

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb reset statistics	Resets SLB statistics for all clusters.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.
ip slb cluster probe	Configures a probe for an SLB cluster.

MIB Objects

```
slbClusterTable
   slbClusterName
   slbClusterVIP
   slbClusterAdminStatus
   slbClusterOperStatus
   slbClusterUpTime
   slbClusterPingPeriod
   slbClusterPingTimeout
   slbClusterPingRetries
   slbClusterRedirectAlgorithm
   slbClusterIdleTimer
   slbClusterNumberOfServers
   slbClusterProbeName
   slbClusterRowStatus
   slbClusterPackets
   slbClusterCondition
   slbClusterType
slbServerTable
   slbServerClusterName
   slbServerIpAddress
   slbServerAdminStatus
   slbServerOperStatus
slbStatsTable
   slbStatsClusterName
   slbStatsIndex
   slbStatsCounter
slbStatsQualTable
   slbStatsQualType
   slbStatsQualData
```

show ip slb cluster server

Displays detailed statistics and configuration information for a single physical server in a Server Load Balancing (SLB) cluster.

show ip slb cluster *name* **server** *ip_address*

Syntax Definitions

name	Specifies the name of the SLB cluster.
ip_address	Specifies the IP address for the physical server.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Specifying a value for the *name* and *ip_address* parameters is required.

Examples

```
-> show ip slb cluster Intranet server 128.220.40.4
Cluster cl1
  VIP 128.220.40.205
    Server 128.220.40.4
      Admin status                              : Enabled,
      Oper status                               : In Service,
      Probe                                     = phttp,
      Availability time (%)                     = 95,
      Ping failures                             = 0,
      Last ping round trip time (milliseconds) = 20,
      Probe status                              = ,
```

Output fields are described here:

output definitions

Cluster	The name of the Server Load Balancing (SLB) cluster.
VIP	The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.
Server	The IP address for this physical server.
Admin status	The current administrative status of this physical server (**Enabled** or **Disabled**).

output definitions (continued)

Oper status	The operational state of this server. The possible states are described as follows: • **Disabled** (this server is administratively disabled). • **No Answer** (this server has not responded to ping requests). • **Link Down** (there is a bad connection to this server). • **In Service** (this server is used for SLB cluster client connections). • **Discovery** (the SLB cluster is pinging this physical server). • **Retrying** (the SLB cluster is making another attempt to bring up this server).
Probe	The name of the probe configured for this server.
Availability time (%)	The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (**In Service** plus **Retrying**) versus down time (**No Answer** plus **Link Down**). Please note that the **Disabled** and the initial **Discovery** states are not counted as down time.
Ping failures	The total number of pings that have failed on this physical server.
Last ping round trip time (milliseconds)	The total amount of time (in milliseconds) measured for the last valid ping to this physical server to make a round trip.
Probe status	The status of the probe configured for this server.

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster.

MIB Objects

```
slbClusterTable
   slbClusterVIP
slbServerTable
   slbServerClusterName
   slbServerIpAddress
   slbServerAdminStatus
   slbServerOperStatus
   slbServerMacAddress
   slbServerSlotNumber
   slbServerPortNumber
   slbServerUpTime
   slbServerProbeName
   slbServerLastRTT
   slbServerPingFails
   slbServerProbeStatus
```

show ip slb servers

Displays the status and configurations of all physical servers in Server Load Balancing clusters.

show ip slb servers

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ip slb servers
                                    Admin     Operational     %
IP addr              Cluster Name   Status    Status          Avail
--------------------+--------------+---------+---------------+-----------
128.220.40.4         Intranet       Enabled   In Service      98
128.220.40.5         Intranet       Enabled   Retrying        80
128.220.40.6         FileTransfer   Enabled   No answer       50
128.220.40.7         FileTransfer   Disabled  Disabled        ---
128.220.40.1         WorldWideWeb   Enabled   In Service      100
128.220.40.2         WorldWideWeb   Enabled   Discovery       50
128.220.40.3         WorldWideWeb   Enabled   Link Down       75
```

Output fields are described here:

output definitions

IP addr	The IP address for this physical server.
Cluster Name	The name of the Server Load Balancing (SLB) cluster to which this physical server belongs.
Admin Status	The current administrative status of this physical server (**Enabled** or **Disabled**).

output definitions (continued)

Operational Status	The operational state of this server. The possible states are described as follows: • **Disabled** (this server is administratively disabled). • **No Answer** (this server has not responded to ping requests). • **Link Down** (there is a bad connection to this server). • **In Service** (this server is used for SLB cluster client connections). • **Discovery** (the SLB cluster is pinging this physical server). • **Retrying** (the SLB cluster is making another attempt to bring up this server).
% Avail	The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (**In Service** plus **Retrying**) versus down time (**No Answer** plus **Link Down**). Please note that the **Disabled** and the initial **Discovery** states are not counted as down time.

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb cluster server	Displays the detailed status and configuration of a single physical server in a Server Load Balancing cluster.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster.

MIB Objects

```
slbServers
   slbServerIpAddress
   slbServerClusterName
   slbServerAdminStatus
   slbServerOperStatus
   slbServerFlows
```

show ip slb probes

Displays the configuration of Server Load Balancing (SLB) probes.

show ip slb probes [*probe_name***]**

Syntax Definitions

probe_name	Specifies the name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

If you do not specify the name of an SLB probe then all SLB probes are displayed.

Examples

No probe name is specified:

```
-> show ip slb probes

Probe Name              Period  Retries Timeout Method
------------------------+-------+-------+--------+------
web_server                60000       3   12000   HTTP
mail_server               60000       3    3000   SMTP
mis_servers             3600000       5   24000   Ping
```

Output fields are described here:

output definitions

Probe Name	The user-specified name of the probe.
Period	The period (in seconds) to check the health of servers.
Retries	The number of probe retries before deciding that a server is out of service.
Timeout	The timeout (in seconds) used to wait for probe answers.
Method	The type of probe.

The name of a probe that is not an HTTP/HTTPS probe is specified:

```
-> show ip slb probes mail_server

Probe mail_server
  Type                          = SMTP,
  Period (seconds)              = 60,
  Timeout (milliseconds)        = 3000,
  Retries                       = 3,
  Port                          = 0,
```

The name of an HTTP/HTTPS probe is specified:

```
-> show ip slb probes phttp

Probe phttp
  Type                          = HTTP,
  Period (seconds)              = 60,
  Timeout (milliseconds)        = 3000,
  Retries                       = 3,
  Port                          = 0,
  Username                      = ,
  Password                      = ,
  Expect                        = ,
  Status                        = 200,
  URL                           = /,
```

Output fields are described here:

output definitions

Probe	The user-specified name of the probe.
Type	The type of probe.
Period	The period (in seconds) to check the health of servers.
Timeout	The timeout (in seconds) used to wait for probe answers.
Retries	The number of probe retries before deciding that a server is out of service.
Port	The TCP/UDP port on which the probe is sent.
Username	The configured user name sent to a server as credentials for an HTTP GET operation for the probe.
Password	The configured password for the probe.
Expect	The configured ASCII string used to compare a response from a server to verify the health of the server.
Status	The expected status returned from an HTTP GET to verify the health of a server.
URL	The configured URL sent to a server for an HTTP GET to verify the health of the server.

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
ip slb probe period	Configures the probe period to check the health of servers.
ip slb probe timeout	Configures the timeout used to wait for probe answers.
ip slb probe retries	Configures the number of probe retries before deciding that a server is out of service.
ip slb probe port	Configures the TCP/UDP port that the probe should be sent on.
ip slb probe username	Configures a user name sent to a server as credentials for an HTTP GET operation
ip slb probe password	Configures a password sent to a server as credentials for an HTTP GET to verify the health of the server
ip slb probe expect	Configures an ASCII string used to compare a response from a server to verify the health of the server.
ip slb probe status	Configures the expected status returned from an HTTP GET to verify the health of a server.
ip slb probe url	Configures a URL sent to a server for an HTTP GET to verify the health of the server.

MIB Objects

```
slbProbeTable
   slbProbeName
   slbProbeMethod
   slbProbePeriod
   slbProbeTimeout
   slbProbeRetries
   slbProbePort
   slbProbeHttpUsername
   slbProbeHttpPassword
   slbProbeExpect
   slbProbeHttpStatus
   slbProbeHttpUrl
```

31 IP Multicast Switching Commands

IP Multicast Switching (IPMS) is a one-to-many communication technique employed by emerging applications such as video distribution, news feeds, conferencing, netcasting, and resource discovery (OSPF, RIP2, and BOOTP). Unlike unicast, which sends one packet per destination, multicast sends one packet to all devices in any subnetwork that has at least one device requesting the multicast traffic.

The OmniSwitch IPMS software is compatible with the following RFCs:

RFC 1112 — Host Extensions for IP Multicasting
RFC 2236 — Internet Group Management Protocol, Version 2
RFC 2933 — Internet Group Management Protocol MIB
RFC 3376 — Internet Group Management Protocol, Version 3

The OmniSwitch IPv6MS software is compatible with the following RFCs:

RFC 2710 — Multicast Listener Discovery for IPv6
RFC 3019 — IPv6 MIB for Multicast Listener Discovery Protocol
RFC 3810 — Multicast Listener Discovery Version 2 for IPv6

MIB information for the IPMS and IPv6MS commands is as follows:

Filename: ALCATEL-IND1-IPMS-MIB.mib
Module: alcatelIND1IpmsMIB

The following table summarizes the available IP and IPv6 multicast commands:

ip multicast admin-state	**ipv6 multicast admin-state**
ip multicast flood-unknown	**ipv6 multicast flood-unknown**
ip multicast version	**ipv6 multicast version**
ip multicast port max-group	**ipv6 multicast port max-group**
ip multicast max-group	**ipv6 multicast max-group**
ip multicast static-neighbor	**ipv6 multicast static-neighbor**
ip multicast static-querier	**ipv6 multicast static-querier**
ip multicast static-group	**ipv6 multicast static-group**
ip multicast query-interval	**ipv6 multicast query-interval**
ip multicast last-member-query-interval	**ipv6 multicast last-member-query-interval**
ip multicast query-response-interval	**ipv6 multicast query-response-interval**
ip multicast unsolicited-report-interval	**ipv6 multicast unsolicited-report-interval**
ip multicast router-timeout	**ipv6 multicast router-timeout**
ip multicast source-timeout	**ipv6 multicast source-timeout**
ip multicast querying	**ipv6 multicast querying**
ip multicast robustness	**ipv6 multicast robustness**
ip multicast spoofing	**ipv6 multicast spoofing**
ip multicast spoofing static-source-ip	**ipv6 multicast spoofing static-source-ip**
ip multicast zapping	**ipv6 multicast zapping**
ip multicast querier-forwarding	**ipv6 multicast querier-forwarding**
ip multicast proxying	**ipv6 multicast proxying**
ip multicast helper-address	**ipv6 multicast helper-address**
ip multicast zero-based-query	**ipv6 multicast zero-based-query**
ip multicast forward-mode	**ipv6 multicast forward-mode**
ip multicast update-delay-interval	**ipv6 multicast update-delay-interval**
ip multicast fast-join	**ipv6 multicast fast-join**
ip multicast host-list	**ipv6 multicast host-list**
ip multicast ssm-map	**ipv6 multicast ssm-map**
ip multicast initial-packet-buffer admin-state	**ipv6 multicast initial-packet-buffer admin-state.**
ip multicast initial-packet-buffer max-packet	**ipv6 multicast initial-packet-buffer max-packet**
ip multicast initial-packet-buffer max-flow	**ipv6 multicast initial-packet-buffer max-flow**
ip multicast initial-packet-buffer timeout	**ipv6 multicast initial-packet-buffer timeout**
ip multicast initial-packet-buffer min-delay	**ipv6 multicast initial-packet-buffer min-delay**
ip multicast display-interface-names	**ipv6 multicast display-interface-names**
ip multicast inherit-default-vrf-config	**ipv6 multicast inherit-default-vrf-config**
ip multicast profile	**ipv6 multicast profile**
ip multicast apply-profile	**ipv6 multicast apply-profile**
show ip multicast	**show ipv6 multicast**
show ip multicast port	**show ipv6 multicast port**
show ip multicast forward	**show ipv6 multicast forward**
show ip multicast neighbor	**show ipv6 multicast neighbor**
show ip multicast querier	**show ipv6 multicast querier**
show ip multicast group	**show ipv6 multicast group**
show ip multicast source	**show ipv6 multicast source**
show ip multicast tunnel	**show ipv6 multicast tunnel**
show ip multicast host-list	**show ipv6 multicast host-list**
show ip multicast ssm-map	**show ipv6 multicast ssm-map**
show ip multicast bridge	**show ipv6 multicast bridge**
show ip multicast bridge-forward	**show ipv6 multicast bridge-forward**
show ip multicast bidir-forward	**show ipv6 multicast bidir-forward**
show ip multicast profile	**show ipv6 multicast profile**

ip multicast admin-state

Enables or disables IP Multicast Switching and Routing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] admin-state [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] admin-state**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable IP Multicast Switching.
disable	Disable IP Multicast Switching.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configuration of an IP multicast routing protocol on an IP interface operationally triggers IP Multicast Switching and Routing functionality on any underlying VLAN or SPB service. This occurs regardless of any explicit IPMS configuration, such as attempting to specifically disable IPMS.
- If there is no IP Multicast routing protocol already running on the switch, then the **ip multicast admin-state** or the **ipv6 multicast admin-state** command alone controls IPMS operations.
- Enabling IPMS on individual VLANs or services, as needed, is recommended to conserve switch resources.
- If IPMS is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.

  Note. Globally enabling the IPMS status for the switch only applies to the VLAN domain (does not apply to the service domain). As a result, IPMS must be explicitly enabled or disabled for each SPB service. However, globally disabling IPMS for all SPB services is supported.

- Use the **no** form of this command to restore the IP Multicast Switching and Routing status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ip multicast admin-state enable
-> ip multicast admin-state disable
-> no ip multicast admin-state
-> ip multicast vlan 2 admin-state enable
-> ip multicast vlan 3-5 admin-state disable
-> no ip multicast vlan 2 admin-state
-> no ip multicast vlan 3-5 admin-state
-> ip multicast service 10 admin-state enable
-> ip multicast service 11-15 admin-state disable
-> no ip multicast service 10 admin-state
-> no ip multicast service 11-15 admin-state
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigStatus
```

ip multicast flood-unknown

Enables or disables the flooding unknown multicast traffic for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified. When a traffic flow is first seen on a port. there is a brief period of time where traffic may get dropped before the forwarding information is calculated. When flooding unknown multicast traffic is enabled, no packets are dropped before the forwarding information is available.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] flood-unknown [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] flood-unknown**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable flooding of unknown traffic until it is learned.
disable	Disable flooding of unknown traffic.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If this command function is enabled after the system is up and running, the flooding of unknown multicast traffic only applies to new flows.
- If the flooding of unknown traffic is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- On an OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 6900:
  - The flood unknown behavior configured for any VLAN is enforced only on that VLAN. However, when the behavior is configured with the IPv6 multicast version of this command (**ipv6 multicast flood-unknown**) for any VLAN, the flood unknown behavior is enforced globally across all VLANs.
  - IPv4 multicast snooping for VLANs does not snoop 224.0.0.0/24 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to the excluded IPv4 addresses.
  - When IPv4 multicast snooping is enabled for any service, the flooding of unknown multicast traffic

is unconditionally enforced for all snooping services; this is the only supported flood unknown behavior for services.

– IPv4 multicast snooping for services does not snoop MAC addresses that fall within the range of 01:00:5e:00:00:00/40 and 33:33:00:00:00:00/40 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to the excluded MAC addresses.

- On an OmniSwitch 9900, IPv4 multicast snooping for VLANs or services does not snoop 224.0.0.0/24 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to these excluded IPv4 addresses.
- Use this command to provide an "open failure" strategy for when hardware resource conflicts or software limits prevent the traffic from being registered in the fast path.
- Use the **no** form of this command to restore the flooding of unknown traffic back to the default value (disabled) on the system or the specified VLAN.

Examples

```
-> ip multicast flood-unknown enable
-> ip multicast flood-unknown disable
-> no ip multicast flood-unknown
-> ip multicast vlan 100 flood-unknown enable
-> ip multicast vlan 101-105 flood-unknown enable
-> ip multicast vlan 100 flood-unknown disable
-> no ip multicast vlan 100 flood-unknown
-> no ip multicast vlan 101-105 flood-unknown
-> ip multicast service 10 flood-unknown enable
-> ip multicast service 11-15 flood-unknown enable
-> ip multicast service 10 flood-unknown disable
-> no ip multicast service 10 flood-unknown
-> no ip multicast service 11-15 flood-unknown
```

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigFloodUnknown
```

ip multicast version

Sets the default version of the IGMP protocol on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] version [***version***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] version**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
version	Default IGMP protocol version to run. Valid range is 1–3.

Defaults

parameter	default
version	2

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the default IGMP protocol version on the system and/or the specified VLANs or SPB services.
- If the default IGMP protocol version is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Due to protocol inter-operation requirements, this command specifies only a default version of the IGMP protocol to run.
- Use the **no** form of this command to restore the IGMP multicast version back to the default value (version 2) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, ip multicast version 0).

Examples

```
-> ip multicast version 3
-> ip multicast version 0
-> no ip multicast version
-> ip multicast vlan 2 version 3
-> ip multicast vlan 3-5 version 3
-> ip multicast vlan 2 version 0
-> no ip multicast vlan 2 version
```

```
-> no ip multicast vlan 3-5 version
-> ip multicast service 2 version 3
-> ip multicast service 3-5 version 3
-> ip multicast service 2 version 0
-> no ip multicast service 2 version
-> no ip multicast service 3-5 version
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigVersion
```

ip multicast port max-group

Configures the maximum group limit learned per port or per Service Access Point (SAP) port. The group limit is applicable to all VLAN instances associated with the specified port or all Shortest Path Bridging (SPB) service instances associated with the specified SAP port.

ip multicast {port *chassis/slot/port* **| sap port** *sap_id***} max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

chassis	The chassis identifier.
slot|port	The slot and port number (3/1).
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
num	The maximum IGMP group count. Valid range is 0–4294967295.
none	Disables the maximum group limit configuration.
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request. A leave is not sent to the router for the replaced group.

Defaults

By default, the maximum group limit is set to zero.

parameter	defaults
action	**none**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If group memberships are already registered on a port/VLAN or SAP port/SPB service instance and the group limit is set to a lower value for the instance, the current group memberships are not removed until they expire. The effect of the new lower group limit value is applied when one of the following occurs to help avoid any undetermined behavior:
  - IP multicast memberships are aged out on a port/VLAN or SAP port/SPB service instance.
  - IP multicast memberships are pruned by a leave or when IP multicast is disabled on the specific VLAN or SPB service or globally disabled for the switch.
- If the *num* and **action** parameters are not specified, then the limit is removed.
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, **ip multicast sap port 1/1/23:10 max-group 10 action drop**, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, "Service Manager Commands," for more information.
- IGMP zapping must be enabled when the maximum group limit is enabled and the action is set to drop.
- Configuring a maximum group limit is allowed even when the IP multicast status is disabled.
- The maximum group configuration is applied in the following order of precedence (listed from highest to lowest precedence):
  - Group limit configured for a port or an SPB SAP port.
  - Group limit configured for a specific VLAN or SPB service.
  - Group limit configured for the IPMS profile assigned to a VLAN or SPB service.
  - Group limit configured for a VLAN or SPB service within a specific VRF context.
  - Group limit configured for the IPMS profile assigned to a VLAN or SPB service within a specific VRF context.

Examples

```
-> ip multicast port 1/1/12 max-group 10 action drop
-> ip multicast port 1/1/14 max-group 20 action replace
-> ip multicast port 1/1/14 max-group

-> ip multicast sap port 1/1/23:10 max-group 10 action drop
-> ip multicast sap port 1/1/26:20.200 max-group 20 action replace
-> ip multicast sap port 1/1/16:20.200 max-group
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **sap port** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.
show ip multicast port	Displays the maximum group configuration for VLAN ports or SPB service SAP ports.

MIB Objects

```
alaIpmsIntfTable
   alaIpmsIntfConfigType
   alaIpmsIntfAddressType
   alaIpmsIntfMaxGroupLimit
   alaIpmsIntfMaxGroupExceedAction
```

ip multicast max-group

Configures the maximum group limit learned per port for the specified VLAN, Shortest Path Bridging (SPB) service, or per port on the system if no VLAN or SPB service is specified. The limit is applied to each port that is a member of the given VLAN or SPB service and the specified action is taken when the limit is exceeded.

ip multicast [vlan *vlan_id***[-***vlan_id2***]** | **service** *service_id***[-***service_id2***]] max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
num	The maximum IGMP group count. Valid range is 0–4294967295.
none	Disables the maximum group limit configuration.
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.

Defaults

By default, the maximum group limit is set to zero.

parameter	defaults
action	**none**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a VLAN or SPB service is not specified, this command configures the global maximum group limit applied to all VLAN ports and SPB Service Access Point (SAP) ports.
- If a VLAN is specified, this command configures the maximum group limit learned per port on a VLAN. The limit is applied to each port that is a member of the given VLAN.
- If an SPB service is specified, this command configures the maximum group limit learned per SAP port on a service. The limit is applied to each SAP port that is a member of the given SPB service.
- Configuring a maximum group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN or SAP port/SPB service instance
- If the *num* and **action** parameters are not specified, then the limit is removed.

- The maximum group configuration on a VLAN or SPB service will override the global configuration.
- The maximum group configuration is applied in the following order of precedence (listed from highest to lowest precedence):
  - Group limit configured for a port or an SPB SAP port.
  - Group limit configured for a specific VLAN or SPB service.
  - Group limit configured for the IPMS profile assigned to a VLAN or SPB service.
  - Group limit configured for a VLAN or SPB service within a specific VRF context.
  - Group limit configured for the IPMS profile assigned to a VLAN or SPB service within a specific VRF context.
- IGMP zapping must be enabled when the maximum group limit is enabled and the action is to drop incoming membership requests.

Examples

```
-> ip multicast max-group 10 action drop
-> ip multicast max-group 20 action replace
-> ip multicast max-group
-> ip multicast vlan 10 max-group 10 action drop
-> ip multicast vlan 20 max-group action drop
-> ip multicast vlan 11-15 max-group 10 action replace
-> ip multicast vlan 10 max-group
-> ip multicast vlan 11-15 max-group
-> ip multicast service 5 max-group 10 action drop
-> ip multicast service 20 max-group action drop
-> ip multicast service 10-15 max-group 10 action replace
-> ip multicast service 5 max-group
-> ip multicast service 10-15 max-group
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.
show ip multicast group	Displays the maximum group configuration for all port or VLAN instances of a given port or all ports.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigMaxGroupLimit
   alaIpmsConfigMaxGroupExceedAction
```

ip multicast static-neighbor

Creates a static IGMP neighbor entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

ip multicast static-neighbor vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

ip multicast static-neighbor service *service_id* **sap {port** | **linkagg} {***sap_id***}**

no ip multicast static-neighbor vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ip multicast static-neighbor service *service_id* **sap {port** | **linkagg} {***sap_id***}**

Syntax Definitions

vlan_id	VLAN to include as a static IGMP neighbor.
chassis	The chassis identifier.
slot|*port*	The slot and port number to configure as a static IGMP neighbor.
agg_id	The link aggregate ID number to configure as a static IGMP neighbor.
service_id	SPB service ID to include as a static IGMP neighbor. The valid range is 1–32767. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static neighbor entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an IGMP static neighbor entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive all of the IGMP traffic *and* IPv4 multicast traffic.
- To create an IGMP static neighbor entry on a link aggregate, use the **linkagg** parameter (for example, **ip multicast static-neighbor vlan 2 linkagg 7** or ip **multicast static-neighbor service 10 sap linkagg 10:100**).
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, **ip multicast static-neighbor service 10 sap port 1/1/23:10**, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, "Service Manager Commands," for more information.

Examples

```
-> ip multicast static-neighbor vlan 4 port 1/1/5
-> no ip multicast static-neighbor vlan 4 port 1/1/5
-> ip multicast static-neighbor vlan 4 linkagg 7
-> no ip multicast static-neighbor vlan 4 linkagg 7

-> ip multicast static-neighbor service 10 sap port 1/1/2:100
-> no ip multicast static-neighbor service 10 sap port 1/1/2:100
-> ip multicast static-neighbor service 10 sap linkagg 10:100
-> no ip multicast static-neighbor service 10 sap linkagg 10:100
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was introduced.
Release 8.4.1; **service** and **sap** parameters added.

Related Commands

show ip multicast neighbor	Displays the IGMP neighbor table entries of IP Multicast Switching and Routing.

MIB Objects

```
alaIpmsStaticNeighborTable
   alaIpmsStaticNeighborConfigType
   alaIpmsStaticNeighborAddressType
   alaIpmsStaticNeighborValue
   alaIpmsStaticNeighborIfIndex
   alaIpmsStaticNeighborSubValue
   alaIpmsStaticNeighborRowStatus
```

ip multicast static-querier

Creates a static IGMP querier entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

ip multicast static-querier vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

ip multicast static-querier service *service_id* **sap {port** | **linkagg} {***sap_id***}**

no ip multicast static-querier vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ip multicast static-querier service *service_id* **sap {port** | **linkagg} {***sap_id***}**

Syntax Definitions

vlan_id	VLAN to include as a static IGMP querier.
chassis	The chassis identifier.
slot|*port*	The slot and port number to configure as a static IGMP querier.
agg_id	The link aggregate ID number to configure as a static IGMP querier.
service_id	SPB service ID to include as a static IGMP querier. The valid range is 1–32767. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static querier entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an IGMP static querier entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive all of the IGMP traffic.
- To create an IGMP static querier entry on a link aggregate, use the **linkagg** parameter (for example, **ip multicast static-querier vlan 2 linkagg 7** or **ip multicast static-querier service 10 sap linkagg 10:100**).
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, **ip multicast static-querier service 10 sap port 1/1/23:10**, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, "Service Manager Commands," for more information.

Examples

```
-> ip multicast static-querier vlan 4 port 1/1/2
-> no ip multicast static-querier vlan 4 port 1/1/2
-> ip multicast static-querier vlan 4 linkagg 7
-> no ip multicast static-querier vlan 4 linkagg 7

-> ip multicast static-querier service 10 sap port 1/1/2:100
-> no ip multicast static-querier service 10 sap port 1/1/2:100
-> ip multicast static-querier service 10 sap linkagg 10:100
-> no ip multicast static-querier service 10 sap linkagg 10:100
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.
Release 8.4.1; **service** and **sap** parameters added.

Related Commands

show ip multicast querier	Displays the IGMP querier table entries of IP Multicast Switching and Routing.

MIB Objects

```
alaIpmsStaticQuerierTable
   alaIpmsStaticQuerierConfigType
   alaIpmsStaticQuerierAddressType
   alaIpmsStaticQuerierValue
   alaIpmsStaticQuerierIfIndex
   alaIpmsStaticQuerierSubValue
   alaIpmsStaticQuerierRowStatus
```

ip multicast static-group

Creates a static IGMP group entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

ip multicast static-group *ip_address* **vlan** *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

ip multicast static-group *ip_address* **service** *service_id* **sap {port** | **linkagg} {***sap_id***}**

no ip multicast static-group *ip_address* **vlan** *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ip multicast static-group *ip_address* **service** *service_id* **sap {port** | **linkagg} {***sap_id***}**

Syntax Definitions

ip_address	The IP address of the multicast group.
vlan_id	VLAN to include as a static IGMP group.
chassis	The chassis identifier.
slot|port	The slot and port number to configure as a static IGMP group.
agg_id	The link aggregate ID number to configure as a static IGMP group.
service_id	SPB service ID to include as a static IGMP group. The valid range is 1–32767. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IGMP static group entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an IGMP static group entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive IGMP traffic addressed to the specified IP multicast group address.
- To create an IGMP static group entry on a link aggregate, use the **linkagg** parameter (for example, ip multicast static-group 225.0.0.1 vlan 2 linkagg 7 or ip multicast static-group 225.0.0.1 service 10 sap linkagg 10:100).
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ip multicast static-querier service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, "Service Manager Commands," for more information.

Examples

```
-> ip multicast static-group 229.10.10.10 vlan 4 port 1/1/2
-> no ip multicast static-group 229.10.10.10 vlan 4 port 1/1/2
-> ip multicast static-group 225.11.11.11 vlan 4 linkagg 7
-> no ip multicast static-group 225.11.11.11 vlan 4 linkagg 7

-> ip multicast static-group 229.10.10.10 service 10 sap port 1/1/2:100
-> no ip multicast static-group 229.10.10.10 service 10 sap port 1/1/2:100
-> ip multicast static-group 225.11.11.11 service 10 sap linkagg 10:100
-> no ip multicast static-group 225.11.11.11 service 10 sap linkagg 10:100
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.
Release 8.4.1; **service** and **sap** parameters added.

Related Commands

show ip multicast group	Displays the IGMP group membership table entries of IP Multicast Switching and Routing for the specified IP multicast group address or all entries if no IP multicast group address is specified.

MIB Objects

```
alaIgmpStaticMemberTable
   alaIpmsStaticMemberConfigType
   alaIpmsStaticMemberAddressType
   alaIpmsStaticMemberValue
   alaIpmsStaticMemberIfIndex
   alaIpmsStaticMemberSubValue
   alaIpmsStaticMemberGroupAddress
   alaIpmsStaticMemberRowStatus
```

ip multicast query-interval

Sets the IGMP query interval on the specified VLAN, Shortest Path Bridging (SPB), or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***] query-interval [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***] query-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
seconds	IGMP query interval in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	125

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP query interval on the system and/or the specified VLANs or SPB services.
- If the IGMP query interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The IGMP query interval refers to the time period between IGMP query messages.
- Due to protocol inter-operation requirements, this command specifies only a default version of the IGMP query interval to use.
- Use the **no** form of this command to restore the IGMP query interval back to the default value (125 seconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, **ip multicast query-interval 0**).

Examples

```
-> ip multicast query-interval 100
-> ip multicast query-interval 0
-> no ip multicast query-interval
-> ip multicast vlan 2 query-interval 100
```

```
-> ip multicast vlan 3-5 query-interval 100
-> ip multicast vlan 2 query-interval 0
-> no ip multicast vlan 2 query-interval
-> no ip multicast vlan 3-5 query-interval
-> ip multicast service 2 query-interval 100
-> ip multicast service 3-5 query-interval 100
-> ip multicast service 2 query-interval 0
-> no ip multicast service 2 query-interval
-> no ip multicast service 3-5 query-interval
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQueryInterval
```

ip multicast last-member-query-interval

Sets the IGMP last member query interval value on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] last-member-query-interval [***tenths_of_seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] last-member-query-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
tenths_of_seconds	IGMP last member query interval in tenths of seconds. The valid range is 1–65535.

Defaults

parameter	default
tenths_of_seconds	10

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP last member query interval on the system and/or the specified VLANs or SPB services.
- If the IGMP last member query interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The IGMP last member query interval refers to the time period to reply to an IGMP query message sent in response to a leave group message.
- Use the **no** form of this command to restore the IGMP last member query interval back to the default value (10 tenth-of-seconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, **ip multicast last-member-query-interval 0**).

Examples

```
-> ip multicast last-member-query-interval 22
-> ip multicast last-member-query-interval 0
-> no ip multicast last-member-query-interval
-> ip multicast vlan 2 last-member-query-interval 22
```

```
-> ip multicast vlan 3-5 last-member-query-interval 22
-> ip multicast vlan 2 last-member-query-interval 0
-> no ip multicast vlan 2 last-member-query-interval
-> no ip multicast vlan 3-5 last-member-query-interval
-> ip multicast service 2 last-member-query-interval 22
-> ip multicast service 3-5 last-member-query-interval 22
-> ip multicast service 2 last-member-query-interval 0
-> no ip multicast service 2 last-member-query-interval
-> no ip multicast service 3-5 last-member-query-interval
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigLastMemberQueryInterval
```

ip multicast query-response-interval

Sets the IGMP query response interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***] query-response-interval [***tenths_of_seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***] query-response-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
tenths_of_seconds	IGMP query response interval in tenths of seconds. The valid range is 1–65535.

Defaults

parameter	default
tenths_of_seconds	100

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP query response interval on the system and/or the specified VLANs or SPB services.
- If the IGMP query response interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The query response interval refers to the time period to reply to an IGMP query message.
- Use the **no** form of this command to restore the IGMP query response interval back to the default value (100 tenths-of-seconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, ip **multicast query-response-interval 0**).

Examples

```
-> ip multicast query-response-interval 200
-> ip multicast query-response-interval 0
-> no ip multicast query-response-interval
-> ip multicast vlan 2 query-response-interval 300
-> ip multicast vlan 3-5 query-response-interval 300
-> ip multicast vlan 2 query-response-interval 0
```

```
-> no ip multicast vlan 2 query-response-interval
-> no ip multicast vlan 3-5 query-response-interval
-> ip multicast service 2 query-response-interval 300
-> ip multicast service 3-5 query-response-interval 300
-> ip multicast service 2 query-response-interval 0
-> no ip multicast service 2 query-response-interval
-> no ip multicast service 3-5 query-response-interval
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQueryReponseInterval
```

ip multicast unsolicited-report-interval

Sets the value of the IGMP unsolicited report interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] unsolicited-report-interval [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] unsolicited-report-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
seconds	IGMP unsolicited report interval in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP unsolicited report interval on the system and/or the specified VLANs or SPB services.
- If the IGMP query response interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The unsolicited report interval refers to the time period to proxy any changed IGMP membership state.
- Use the **no** form of this command to restore the IGMP unsolicited report interval back to the default value (1 second) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, **ip multicast unsolicited-report-interval 0**).

Examples

```
-> ip multicast unsolicited-report-interval 200
-> ip multicast unsolicited-report-interval 0
-> no ip multicast unsolicited-report-interval
-> ip multicast vlan 2 unsolicited-report-interval 300
-> ip multicast vlan 3-5 unsolicited-report-interval 300
-> ip multicast vlan 2 unsolicited-report-interval 0
```

```
-> no ip multicast vlan 2 unsolicited-report-interval
-> no ip multicast vlan 3-5 unsolicited-report-interval
-> ip multicast service 2 unsolicited-report-interval 300
-> ip multicast service 3-5 unsolicited-report-interval 300
-> ip multicast service 2 unsolicited-report-interval 0
-> no ip multicast service 2 unsolicited-report-interval
-> no ip multicast service 3-5 unsolicited-report-interval
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigUnsolicitedReportInterval
```

ip multicast router-timeout

Configures the expiry time of IP multicast routers on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] router-timeout [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] router-timeout**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
seconds	IGMP router timeout in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP router timeout on the system and/or the specified VLANs.
- If the IGMP router timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- Use the **no** form of this command to restore the IGMP router timeout back to the default value (90 seconds) on the system or the specified VLAN. In addition, specifying a value of 0 with this command also restores the default value (for example, **ip multicast router-timeout 0**).

Examples

```
-> ip multicast router-timeout 100
-> ip multicast router-timeout 0
-> no ip multicast router-timeout
-> ip multicast vlan 2 router-timeout 100
-> ip multicast vlan 3-5 router-timeout 100
-> ip multicast vlan 2 router-timeout 0
-> no ip multicast vlan 2 router-timeout
-> no ip multicast vlan 3-5 router-timeout
-> ip multicast service 2 router-timeout 100
-> ip multicast service 3-5 router-timeout 100
```

```
-> ip multicast service 2 router-timeout 0
-> no ip multicast service 2 router-timeout
-> no ip multicast servicee 3-5 router-timeout
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigRouterTimeout
```

ip multicast source-timeout

Configures the expiry time of IP multicast sources on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] source-timeout [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] source-timeout**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
seconds	IGMP source timeout in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP source timeout on the system and/or the specified VLANs.
- If the IGMP source timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- Use the **no** form of this command to restore the IGMP source timeout back to the default value (30 seconds) on the system or the specified VLAN. In addition, specifying a value of 0 with this command also restores the default value (for example, **ip multicast source-timeout 0**).

Examples

```
-> ip multicast source-timeout 100
-> ip multicast source-timeout 0
-> no ip multicast source-timeout
-> ip multicast vlan 2 source-timeout 100
-> ip multicast vlan 3-5 source-timeout 100
-> ip multicast vlan 2 source-timeout 0
-> no ip multicast vlan 2 source-timeout
-> no ip multicast vlan 3-5 source-timeout 100
-> ip multicast service 2 source-timeout 100
-> ip multicast service 3-5 source-timeout 100
```

```
-> ip multicast service 2 source-timeout 0
-> no ip multicast service 2 source-timeout
-> no ip multicast service 3-5 source-timeout
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigSourceTimeout
```

ip multicast querying

Enables or disables IGMP querying on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] querying {enable | disable} [static-source-ip** *ip_address***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***]] querying [static-source-ip]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
enable	Enable IGMP querying.
disable	Disable IGMP querying.
ip_address	A static source IPv4 address to use for IGMP querying. *This parameter is currently not supported.*

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to enable IGMP querying on the system and/or specified VLANs.
- If the IGMP querying is already enabled/disabled on the system, then the VLAN configuration will override the system's configuration.
- IGMP querying refers to requesting the network's IGMP group membership information by sending out IGMP queries. IGMP querying also involves participating in IGMP querier election.
- Use the **no** form of this command to restore the IGMP querying status to the default value (disabled) on the system or the specified VLAN.

Examples

```
-> ip multicast querying enable
-> ip multicast querying disable
-> no ip multicast querying
-> ip multicast vlan 2 querying enable
-> ip multicast vlan 3-5 querying disable
-> no ip multicast vlan 2 querying
-> no ip multicast vlan 3-5 querying
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1.R02; **static-source-ip** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQuerying
   alaIpmsConfigQueryingStaticSourceAddress
```

ip multicast robustness

Sets the IGMP robustness variable on the specified VLAN, Shortest Path Bridging (SPB) service or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] robustness [***robustness***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] robustness**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
robustness	IGMP robustness variable. Valid range is 1–7.

Defaults

parameter	default
robustness	2

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP robustness variable on the system and/or the specified VLANs or SPB services.
- If the IGMP robustness variable is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Robustness variable allows fine-tuning on the network, where the expected packet loss would be greater.
- Due to protocol inter-operation requirements, this command specifies only a default version of the IGMP robustness variable to use.
- Use the **no** form of this command to restore the IGMP robustness variable back to the default value (2) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, ip multicast robustness 0).

Examples

```
-> ip multicast robustness 3
-> ip multicast robustness 0
-> no ip multicast robustness
-> ip multicast vlan 2 robustness 3
```

```
-> ip multicast vlan 3-5 robustness 3
-> ip multicast vlan 2 robustness 0
-> no ip multicast vlan 2 robustness
-> no ip multicast vlan 3-5 robustness
-> ip multicast service 2 robustness 3
-> ip multicast service 3-5 robustness 3
-> ip multicast service 2 robustness 0
-> no ip multicast service 2 robustness
-> no ip multicast service 3-5 robustness
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigRobustness
```

ip multicast spoofing

Enables or disables IGMP spoofing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] spoofing {enable | disable}**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] spoofing**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, OmniSwitch 6900-V72.*
enable	Enable IGMP spoofing.
disable	Disable IGMP spoofing.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IGMP spoofing configuration and return the specified VLAN, SPB service, or system to the default behavior.
- If the IGMP spoofing is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- IGMP spoofing refers to replacing a client source MAC and IP address with the system's MAC and IP address when relaying or proxying aggregated IGMP group membership information to other devices.
- By default, the source IP address is not specified for spoofing; the system determines these addresses automatically. Optionally configure a static source IP address using the **ip multicast spoofing static-source-ip** command to overcome the need for an IP interface. If configured, the static source IP is always used for spoofing, regardless of the IP interface address or administrative state.

Examples

```
-> ip multicast spoofing enable
-> ip multicast spoofing disable
-> no ip multicast spoofing
-> ip multicast vlan 2 spoofing enable
```

```
-> ip multicast vlan 3-5 spoofing disable
-> no ip multicast vlan 2 spoofing
-> no ip multicast vlan 3-5 spoofing
-> ip multicast service 2 spoofing enable
-> ip multicast service 3-5 spoofing disable
-> no ip multicast service 2 spoofing
-> no ip multicast service 3-5 spoofing
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigSpoofing
```

ip multicast spoofing static-source-ip

Configures an IGMP static spoofing address on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] spoofing static-source-ip** *ip_address*

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] spoofing static-source-ip**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
ip_address	A static source IPv4 address to use for spoofing.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a static source IP address.
- IGMP spoofing refers to replacing a client source MAC and IP address with the system's MAC and IP address when relaying or proxying aggregated IGMP group membership information to other devices.
- By default, a source IP address is not specified when spoofing is enabled. As a result, the switch will automatically use the address of the IP interface associated with the LAN. If there is no IP interface address to use, the switch will then use the Loopback0 interface address associated with the current VRF instance.
- Use this command to optionally configure a static source IP address to overcome the need for an IP interface. If configured, the static source IP is always used for spoofing, regardless of the IP interface address or administrative state.

Examples

```
-> ip multicast spoofing static-source-ip 10.2.2.1
-> no ip multicast spoofing static-source-ip
-> ip multicast vlan 2 spoofing static-source-ip 10.2.2.1
-> ip multicast vlan 3-5 spoofing static-source-ip 10.2.2.1
-> no ip multicast vlan 2 spoofing static-source-ip
-> no ip multicast vlan 3-5 spoofing static-source-ip
-> ip multicast service 2 spoofing static-source-ip 11.2.2.1
```

```
-> no ip multicast service 2 spoofing static-source-ip
-> ip multicast service 3-5 spoofing static-source-ip 11.2.2.1
-> no ip multicast service 3-5 spoofing static-source-ip
```

Release History

Release 8.3.1.R02; command was added.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigSpoofingStaticSourceAddress
```

ip multicast zapping

Enables or disables IGMP zapping on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***] zapping [{enable | disable}]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] zapping**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable IGMP zapping.
disable	Disable IGMP zapping.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the IGMP zapping is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- IGMP zapping refers to processing membership, immediate source filter removals and will not wait for the protocol's specified time period. This mode facilitates IP TV applications looking for quick changes between IP multicast groups.
- Use the **no** form of this command to restore the IGMP zapping status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ip multicast zapping enable
-> ip multicast zapping disable
-> no ip multicast zapping
-> ip multicast vlan 2 zapping enable
-> ip multicast vlan 3-5 zapping disable
-> no ip multicast vlan 2 zapping
-> no ip multicast vlan 3-5 zapping
-> ip multicast service 2 zapping enable
```

```
-> ip multicast service 3-5 zapping disable
-> no ip multicast service 2 zapping
-> no ip multicast service 3-5 zapping
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigZapping
```

ip multicast querier-forwarding

Enables or disables IGMP querier forwarding on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] querier-forwarding [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] querier-forwarding**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable IGMP querier forwarding.
disable	Disable IGMP querier forwarding.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the IGMP querier forwarding is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- IGMP querier forwarding refers to promoting detected IGMP queriers to receive all IP multicast data traffic.
- Use the **no** form of this command to restore the IGMP querier forwarding status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ip multicast querier-forwarding enable
-> ip multicast querier-forwarding disable
-> no ip multicast querier-forwarding
-> ip multicast vlan 2 querier-forwarding enable
-> ip multicast vlan 3-5 querier-forwarding disable
-> no ip multicast vlan 2 querier-forwarding
-> no ip multicast vlan 3-5 querier-forwarding
-> ip multicast service 2 querier-forwarding enable
```

```
-> ip multicast service 3-5 querier-forwarding disable
-> no ip multicast service 2 querier-forwarding
-> no ip multicast service 3-5 querier-forwarding
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQuerierForwarding
```

ip multicast proxying

Enables or disables IGMP proxying on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] proxying [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] proxying**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable IGMP proxying.
disable	Disable IGMP proxying.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the IGMP proxying is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- IGMP proxying refers to processing membership information on behalf of client systems and reporting membership on their behalf.
- Proxy reported IGMP packets are sent using the source MAC address of the proxying switch. Unless the spoofing feature is used, proxy reported IGMP packets will be sent using 0.0.0.0 for the IPv4 source address.
- Use the **no** form of this command to restore the IGMP proxying status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ip multicast proxying enable
-> ip multicast proxying disable
-> no ip multicast proxying
-> ip multicast vlan 2 proxying enable
-> ip multicast vlan 3-5 proxying disable
-> no ip multicast vlan 2 proxying
-> no ip multicast vlan 3-5 proxying
-> ip multicast service 2 proxying enable
-> ip multicast service 3-5 proxying disable
-> no ip multicast service 2 proxying
-> no ip multicast service 3-5 proxying
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigProxying
```

ip multicast helper-address

Specifies the destination IP address of a relay host where IGMP host Reports and Leave messages are sent.

ip multicast [vlan *vlan_id***[-***vlan_id2***] helper-address** *ip_address*

no ip multicast [vlan *vlan_id***[-***vlan_id2***] helper-address**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
ip_address	The IP address of the relay host.

Defaults

parameter	default
ip_address	0.0.0.0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- After the destination IP address is specified, the IPMS reporting feature is enabled.
- An operational IPv4 interface is required for the receiving LAN before any IGMP Reports and Leave messages can be relayed.
- Configuring a destination IP helper address is supported only in the VLAN domain; the service domain is not supported.
- Use the **no** form of this command to restore the IPMS reporting feature back to the default value (IP address 0.0.0.0) on the system. When the IP address is set to 0.0.0.0, the IPMS reporting feature is disabled.

Examples

```
-> ip multicast helper-address 10.1.1.198
-> no ip multicast helper-address
-> ip multicast vlan 2 helper-address 10.1.1.198
-> ip multicast vlan 3-5 helper-address 10.1.1.198
-> no ip multicast vlan 2 helper-address
-> no ip multicast vlan 3-5 helper-address
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters,

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigHelperAddress
```

ip multicast zero-based-query

Configures the use of an all-zero source IPv4 address for IGMP query packets when a non-querier is querying the membership of a port. This value is set for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] zero-based-query [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] zero-based-query**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable IGMP zero-based querying.
disable	Disable IGMP zero-based querying.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The IGMP zero-based query status set for a specific VLAN or SPB service overrides the zero-based query status set for the system.
- Use the **no** form of this command to restore the IGMP zero-based query status back to the default value (enabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ip multicast zero-based-query enable
-> ip multicast zero-based-query disable
-> no ip multicast zero-based-query
-> ip multicast vlan 2 zero-based-query enable
-> ip multicast vlan 3-5 zero-based-query disable
-> no ip multicast vlan 2 zero-based-query
-> no ip multicast vlan 3-5 zero-based-query
-> ip multicast service 10 zero-based-query enable
-> ip multicast service 10-15 zero-based-query disable
-> no ip multicast service 10 zero-based-query
```

```
-> no ip multicast service 10-15 zero-based-query disable
```

Release History

Release 8.3.1; command introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigZeroBasedQuery
```

ip multicast forward-mode

Configures the Layer 2 forwarding mode for IPv4 Multicast Switching (does not apply to IPv4 Multicast Routing).The forwarding mode is set for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] forward-mode {asm | ssm | mac | auto}**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] forward-mode**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
asm	Sets the IPMS forwarding mode to ASM (the bridge lookup is based on the packet group destination IP address). *This parameter is supported only in the VLAN domain; service domain is not supported.*
ssm	Sets the IPMS forwarding mode to SSM (the bridge lookup is based on the packet source IP as well as the group destination IP). *This parameter is supported only in the VLAN domain; service domain is not supported*
mac	Sets the IPMS forwarding mode to MAC address (the bridge lookup is based on the MAC destination address).
auto	Automatically determines the IPMS forwarding mode based on the current IGMP protocol version and the existing protocol state.

Defaults

By default, the forwarding mode is set to automatic.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The forwarding mode set for a specific VLAN or SPB service overrides the forwarding mode set for the system.
- If multicast routing is enabled on a VLAN, the following conditions apply:
  - On the OmniSwitch 9900, the bridging mode is independent of the routing mode. As a result, ASM bridging is allowed in a VLAN that has SSM routing configured or SSM bridging is allowed in a VLAN that has ASM routing configured.
  - Multicast routing is not supported on the OmniSwitch 6560.

  - On all other OmniSwitch platforms, the routing configuration overrides the forwarding mode setting and determines the forwarding mode based on the group mappings. For example, BIDIR flows will use ASM while DVMRP flows and all other PIM modes will use SSM.

- Use the **no** form of this command to restore the Layer 2 forwarding mode back to the default value (automatic) on the system or the specified VLAN or SPB service.

Examples

```
-> ip multicast forward-mode auto
-> ip multicast forward-mode asm
-> ip multicast forward-mode ssm
-> ip multicast forward-mode mac
-> no ip multicast forward-mode
-> ip multicast vlan 100 forward-mode auto
-> ip multicast vlan 101-104 forward-mode asm
-> ip multicast vlan 100 forward-mode ssm
-> ip multicast vlan 101-104 forward-mode mac
-> no ip multicast vlan 100 forward-mode
-> no ip multicast vlan 101-104 forward-mode
-> ip multicast service 10 forward-mode mac
-> ip multicast service 11-15 forward-mode mac
-> no ip multicast service 10 forward-mode
-> no ip multicast service 11-15 forward-mode
```

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.
show ip multicast bridge	Displays the forwarding mode for IP multicast bridge table entries.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigForwardMode
```

ip multicast update-delay-interval

Sets the amount of time to delay IPv4 multicast forwarding updates on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] update-delay-interval** *milliseconds*

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] update-delay-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
milliseconds	The number of milliseconds to defer forwarding updates. Valid range is 0–10000.

Defaults

By default, the forwarding update delay interval is set to zero.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the forwarding update delay is set to zero, forwarding updates are processed immediately with minimal latency. Configuring a forwarding update delay value can limit the effects of persistent churn on the system.
- If the forwarding update delay interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Use the **no** form of this command to restore the forwarding update delay interval back to the default value (zero) on the system or the specified VLAN or SPB service.

Examples

```
-> ip multicast update-delay-interval 10
-> no ip multicast update-delay-interval
-> ip multicast vlan 100 update-delay-interval 20
-> ip multicast vlan 101-105 update-delay-interval 20
-> no ip multicast vlan 100 update-delay-interval
-> no ip multicast vlan 101-105 update-delay-interval
-> ip multicast service 20 update-delay-interval 20
-> ip multicast service 21-25 update-delay-interval 20
-> no ip multicast service 20 update-delay-interval
-> no ip multicast service 21-25 update-delay-interval
```

Release History

Release 8.3.1; command was introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigUpdateDelayInterval
```

ip multicast fast-join

Configures whether or not IP Multicast Switching will automatically create the forwarding entries in hardware as soon as the IGMP memberships are learned on the specified VLAN, Shortest Path Bridging (SPB) service or globally if no VLAN or SPB service is specified.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] fast-join [enable | disable]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] fast-join**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs. *This parameter is supported only on the OmniSwitch 9900.*
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6900-C32 or OmniSwitch 6900-V72.*
enable	Enable the IGMP fast join functionality.
disable	Disable the IGMP fast join functionality.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command applies only to IPv4 Multicast Switching. If IP Multicast Routing is enabled, then the routing configuration will override the fast join setting.
- When the IP Multicast Switching fast join functionality is enabled, convergence of multicast traffic may occur faster because the forwarding entries are already created before the actual multicast traffic is received.
- When the IP Multicast Switching fast join functionality is disabled (the default), forwarding entries are not created in the hardware until the multicast traffic reaches the switch.
- If the IP Multicast Switching fast join is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Use the **no** form of this command to restore the IP Multicast Switching fast join setting back to the default value (disabled) on the system or the specified VLAN or SPB service.

Examples

```
-> ip multicast fast-join enable
-> ip multicast fast-join disable
-> no ip multicast fast-join
-> ip multicast service 10 fast-join enable
-> ip multicast service 11-15 fast-join disable
-> no ip multicast service 10 fast-join
-> no ip multicast service 11-15 fast-join
```

Release History

Release 8.3.1.R02; command introduced.
Release 8.4.1.R02; **vlan** and **service** parameters added.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigFastJoin
```

ip multicast host-list

Configures a list of host IP addresses that is used for IP multicast group maps and SSM maps.

ip multicast host-list *host_list_name ip_address* **[***ip_address***]**

no ip multicast host-list *host_list_name* **[***ip_address***]**

Syntax Definitions

host_list_name	A name to assign to the host list (up to 20 characters).
ip_address	The IP address to add to the host list. Multiple IP addresses can be entered on the same command line.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Use the **no** form of this command to remove an IP address from the list or remove the entire list from the switch configuration.
- When the entire list is removed, any configuration associated with the list is also removed.

Examples

```
-> ip multicast host-list group-map1 10.1.1.198
-> ip multicast host-list ssm-map1 20.0.0.1
-> ip multicast host-list ssm-map2 30.0.0.1 30.0.0.2 30.0.0.3
-> no ip multicast host-list ssm-map2 30.0.0.2
-> no ip multicast host-list group-map1
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip multicast host-list	Displays the IP multicast host address list configuration for the switch.

MIB Objects

```
alaIpmsHostListTable
   alaIpmsHostListName
   alaIpmsHostListAddressType
   alaIpmsHostListAddress
```

ip multicast ssm-map

Configures the translation of Any Source Multicast (ASM) group memberships into Source Specific Multicast (SSM) group memberships on the specified VLAN or on the system if no VLAN is specified.

ip multicast [vlan *vlan_id***] ssm-map {***group_address/prefixLen host_list_name* | **admin-state {enable | disable}}**

no ip multicast [vlan *vlan_id***] ssm-map** *group_address/prefixLen*

Syntax Definitions

vlan_id	VLAN on which to apply the mapping configuration.
*group_address***[***/prefixLen***]**	The multicast group address/prefix length to map to the host list. If no prefix length is specified, then the a default length of 32 is used.
host_list_name	The name of a host list to use for SSM mapping.
enable	Enables the SSM mapping.
disable	Disables the SSM mapping.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Use the **no** form of this command to remove the SSM mapping configuration from the system or the specified VLAN.
- If an SSM mapping is already enabled on the system, then the VLAN configuration will override the system's configuration.

Examples

```
-> ip multicast ssm-map 229.10.10.10 hostList1
-> ip multicast ssm-map admin-state enable
-> ip multicast vlan 200 ssm-map 225.11.11.11 hostList2
-> ip multicast vlan 200 ssm-map admin-state enable
-> no ip multicast ssm-map 229.10.10.10
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip multicast ssm-map	Displays the SSM mapping configuration.
show ip multicast	Displays the IP Multicast Switching and Routing status and general configuration parameters, such as the SSM mapping setting.

MIB Objects

```
alaIpmsSsmMapTable
   alaIpmsSsmMapConfigType
   alaIpmsSsmMapConfigAddressType
   alaIpmsSsmMapConfigValue
   alaIpmsSsmMapGroupAddress
   alaIpmsSsmMapGroupPrefixLength
   alaIpmsSsmMapSourceListName
```

ip multicast initial-packet-buffer admin-state

Enables or disables initial packet buffering for IPv4 multicast flows on the specified VLAN or globally on the switch.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer admin-state {enable | disable}**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
enable	Enable the initial packet buffering globally on the switch.
disable	Disable the initial packet buffering globally on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- When enabled, the following configuration is used for initial packet buffering on new multicast flows:
  - The maximum number of initial packets buffered per IPv4 multicast flow. Use the **ip multicast initial-packet-buffer max-packet** command to set this value.
  - The maximum number of IPv4 multicast flows that can be buffered. Use the **ip multicast initial-packet-buffer max-flow** command to set this value.
  - The maximum amount of time buffered packets are held if they are not sent out. Use the **ip multicast initial-packet-buffer timeout** command to set this value.
  - The minimum amount of time packets are held before delivery begins. Use the **ip multicast initial-packet-buffer min-delay** command to set this value.
- Configuring the status for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ip multicast initial-packet-buffer admin-state disable
-> ip multicast vlan 2 initial-packet-buffer admin-state enable
-> ip multicast vlan 3-5 initial-packet-buffer admin-state enable
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBuffer
```

ip multicast initial-packet-buffer max-packet

Configures the maximum number of initial packets buffered per IPv4 multicast flow on the specified VLAN or globally on the switch.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer max-packet [***num***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
num	The maximum number of packets allowed to buffer per IPv4 multicast flow. Valid range is 1–10.

Defaults

parameter	default
num	4

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ip multicast initial-packet-buffer max-packet 4
-> ip multicast vlan 2 initial-packet-buffer max-packet 10
-> ip multicast vlan 3-5 initial-packet-buffer max-packet 10
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

ip multicast initial-packet-buffer admin-state	Enables or disables the initial packet buffering feature globally on the switch for IPv4 multicast flows.
show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferMaxPacket
```

ip multicast initial-packet-buffer max-flow

Configures the maximum number of IPv4 multicast flows that can be buffered on the specified VLAN or globally on the switch.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer max-flow [***num***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
num	The maximum number of IPv4 multicast flows allowed for initial packet buffering. Valid range is 1–32.

Defaults

parameter	default
num	32

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ip multicast initial-packet-buffer max-flow 32
-> ip multicast vlan 2 initial-packet-buffer max-flow 32
-> ip multicast vlan 3-5 initial-packet-buffer max-flow 32
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

ip multicast initial-packet-buffer admin-state	Enables or disables the initial packet buffering feature globally on the switch for IPv4 multicast flows.
show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferMaxFlow
```

ip multicast initial-packet-buffer timeout

Configures the timeout value for the buffered IPv4 initial multicast packets on the specified VLAN or globally on the switch.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer timeout [***seconds***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
seconds	The timeout value for the initial buffered IPv4 multicast packets in seconds. Valid range is 1–10.

Defaults

parameter	default
seconds	10

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- If the buffered multicast packet is not sent out before the timeout, then the buffered packets will be removed from IPMS system.
- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ip multicast initial-packet-buffer timeout 2
-> ip multicast vlan 2 initial-packet-buffer timeout 5
-> ip multicast vlan 3-5 initial-packet-buffer timeout t
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

ip multicast initial-packet-buffer admin-state	Enables or disables the initial packet buffering feature globally on the switch, for IPv4 multicast flows.
show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferTimeout
```

ip multicast initial-packet-buffer min-delay

Configures the minimum delay to program the multicast replication index for IPv4 multicast flows buffered for initial packet on the specified VLAN or globally on the switch.

ip multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer min-delay [***milliseconds***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
milliseconds	The minimum delay value to program the multicast replication index for IPv4 multicast flows buffered for initial packet. Valid range is 0–1000.

Defaults

parameter	default
milliseconds	0

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

Note. This command configures a timer to delay the programming of multicast replication index in hardware which might increase the number of multicast packets lost during the learning phase.

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ip multicast initial-packet-buffer min-delay 200
-> ip multicast vlan 2 initial-packet-buffer min-delay 200
-> ip multicast vlan 3-5 initial-packet-buffer min-delay 200
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

ip multicast initial-packet-buffer admin-state	Enables or disables the initial packet buffering feature globally on the switch for IPv4 multicast flows.
show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferMinDelay
```

ip multicast display-interface-names

Sets the display output of the **show** commands listed below. When enabled, the display outputs for these commands will show the IP interface name for each VLAN associated with the IP multicast table entry.

ip multicast display-interface-names

no ip multicast display-interface-names

Syntax Definitions

N/A

Defaults

By default, this function is disabled. The display format is set to include the VLANs that are associated with the IP multicast source and forward flows.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to revert back to displaying the VLAN name.
- If there are any VLANs that are not configured with an IP interface or the IP interface is disabled, the output display will still include the VLAN when this function is enabled.
- This command may be helpful when reviewing output from multicast snooping commands and comparing state in multicast routing, which only interacts with IP interfaces.
- Enabling the display interface names option applies to the following **show** commands:

  show ip multicast forward
  show ip multicast neighbor
  show ip multicast querier
  show ip multicast group
  show ip multicast source
  show ip multicast tunnel

- The command examples provided display the **show ip multicast source** output after the display interface name function is turned on (enabled) and off (disabled).

Examples

```
-> ip multicast display-interface-name
-> show ip multicast source

Total 11 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
--------------+--------------+---------------+--------------
239.192.1.17    172.1.1.1       0.0.0.0         VL-10
239.192.1.18    172.1.1.2       0.0.0.0         VL-10
239.192.1.19    172.1.1.3       0.0.0.0         VL-10
239.192.1.20    172.1.1.4       0.0.0.0         VL-10
239.192.1.21    172.1.1.5       0.0.0.0         VL-10
239.192.1.22    172.1.1.6       0.0.0.0         VL-10
239.192.1.23    172.1.1.7       0.0.0.0         VL-10
239.192.1.24    172.1.1.8       0.0.0.0         VL-10
239.192.1.25    172.1.1.9       0.0.0.0         VL-10
239.192.1.9     173.1.1.9       0.0.0.0         VL-20
239.192.1.10    173.1.1.10      0.0.0.0         VL-20

-> no ip multicast display-interface-name
-> show ip multicast source

Total 11 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
--------------+--------------+---------------+--------------
239.192.1.17    172.1.1.1       0.0.0.0         vlan 1001
239.192.1.18    172.1.1.2       0.0.0.0         vlan 1001
239.192.1.19    172.1.1.3       0.0.0.0         vlan 1001
239.192.1.20    172.1.1.4       0.0.0.0         vlan 1001
239.192.1.21    172.1.1.5       0.0.0.0         vlan 1001
239.192.1.22    172.1.1.6       0.0.0.0         vlan 1001
239.192.1.23    172.1.1.7       0.0.0.0         vlan 1001
239.192.1.24    172.1.1.8       0.0.0.0         vlan 1001
239.192.1.25    172.1.1.9       0.0.0.0         vlan 1001
239.192.1.9     173.1.1.9       0.0.0.0         vlan 2001
239.192.1.10    173.1.1.10      0.0.0.0         vlan 2001
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip multicast source	Displays the IP Multicast Switching and Routing source table entries.
show ip multicast forward	Displays the IP Multicast Switching and Routing forwarding table entries.

MIB Objects

```
alaIpmsGlobalConfigTable
   alaIpmsGlobalConfigAddressType
   alaIpmsGlobalConfigDisplayInterfaceNames
```

ip multicast inherit-default-vrf-config

Configures whether or not the global IPMS configuration defined in the default VRF instance is applied to all VRF instances.

ip multicast inherit-default-vrf-config

no ip multicast inherit-default-vrf-config

Syntax Definitions

N/A

Defaults

By default, the global IPMS configuration defined in the default VRF instance is applied to all VRF instances on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this function. When disabled, the global IPMS configuration defined in the default VRF instance is not applied to all other VRF instances on the switch.
- When enabled (the default), additional VRF instances will inherit the global IPMS configuration defined in the default VRF instance.
- A global IPMS configuration defined for a specific non-default VRF instance takes precedence over the global IPMS configuration defined for the default VRF.
- Note that any per-VLAN IPMS configuration defined in a non-default VRF instance will show up as part of the default VRF instance in the configuration snapshot file. However, the functionality is still applied within the context of VRF instance in which the per-VLAN configuration was originally defined.

Examples

```
-> ip multicast inherit-default-vrf-config
-> no ip multicast inherit-default-vrf-config
```

Release History

Release 8.3.1; command introduced.

Related Commands

show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

MIB Objects

```
alaIpmsGlobalConfigTable
   alaIpmsGlobalConfigAddressType
   alaIpmsGlobalConfigInheritDefaultVrfConfig
```

ip multicast profile

Defines an IPMS profile that is used to apply a pre-defined configuration to the global IPMS instance (all VLAN and service instances) or to a specific VLAN or service instance. Using a configuration profile to configure IPMS functionality avoids having to configure each IPMS parameter with a separate CLI command.

This section describes the base command (**ip multicast profile**) along with optional command keywords that are used to configure IPMS parameter values that are applied when the profile is assigned to an IPMS instance. Optional keywords are listed separately but can be entered in combination on the same command line. Use the **no** form for the keywords to change a specific parameter value for the profile.

There is a "default" profile that defines a default set of IPMS parameter values that is automatically assigned to an IPMS instance. The default profile cannot be deleted, but the profile parameter values are configurable through this command.

ip multicast profile *profile_name*
[admin-state {enable | disable}]
[flood-unknown {enable | disable}]
[version *version***]**
[robustness *robustness***]**
[querying {enable | disable}]
[query-interval [*seconds***]]**
[query-response-interval [*tenths-of-seconds***]]**
[last-member-query-interval [*tenths-of-seconds***]]**
[unsolicited-report-interval [*seconds***]]**
[proxying {enable | disable}]
[spoofing {enable | disable}]
[spoofing static-source-ip *ip_address***]**
[zapping {enable | disable}]
[querier-forwarding {enable | disable}]
[router-timeout [*seconds***]]**
[source-timeout [*seconds***]]**
[max-group [*num***] [action {none | drop | replace}]]**
[helper-address [*ip_address***]]**
[zero-based-query {enable | disable}]
[forward-mode {asm | ssm | mac | auto}
[update-delay-interval *milliseconds***]**
[fast-join {enable | disable}]
[initial-packet-buffer admin-state {enable | disable}]
[initial-packet-buffer max-flow [*num***]]**
[initial-packet-buffer max-packet [*num***]]**
[initial-packet-buffer timeout [*seconds***]**
[initial-packet-buffer min-delay [milliseconds]

no ip multicast profile *profile_name* **[admin-state | flood-unknown | version | robustness | ...]**

Syntax Definitions

profile_name The name to associate with the IPMS profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IPMS profile from the switch configuration.
- To change the value of a specific profile parameter, specify the parameter keyword with this command. For example, **no ip multicast profile ipms-1 admin-state**, **ip multicast profile ipms-1 query-interval 100**, or **ip multicast profile ipms-1 querying enable**. The new parameter values are applied to all IPMS instances to which the profile is assigned.
- The profile name must already exist in the switch configuration before parameter values can be modified. Use this command to create the profile first, then configure the profile parameter values.
- For more information about specific profile parameter values, refer to the following explicit IPMS configuration commands for each profile parameter:

Port Template Parameter	Explicit Port Configuration Command
[admin-state {enable | disable}]	**ip multicast admin-state**
[flood-unknown {enable | disable}]	**ip multicast flood-unknown**
[version *version***]**	**ip multicast version**
[robustness *robustness***]**	**ip multicast robustness**
[querying {enable | disable}]	**ip multicast querying**
[query-interval [*seconds***]]**	**ip multicast query-interval**
[query-response-interval [*tenths-of-seconds***]]**	**ip multicast query-response-interval**
[last-member-query-interval [*tenths-of-seconds***]]**	**ip multicast last-member-query-interval**
[unsolicited-report-interval [*seconds***]]**	**ip multicast unsolicited-report-interval**
[proxying {enable | disable}]	**ip multicast proxying**
[spoofing {enable | disable}]	**ip multicast spoofing**
[spoofing static-source-ip *ip_address***]**	**ip multicast spoofing static-source-ip**
[zapping {enable | disable}]	**ip multicast zapping**
[querier-forwarding {enable | disable}]	**ip multicast querier-forwarding**
[router-timeout [*seconds***]]**	**ip multicast router-timeout**
[source-timeout [*seconds***]]**	**ip multicast source-timeout**
[max-group [*num***] [action {none | drop | replace}]]**	**ip multicast max-group**

Port Template Parameter	Explicit Port Configuration Command
[helper-address [*ip_address***]]**	**ip multicast helper-address**
[zero-based-query {enable | disable}]	**ip multicast zero-based-query**
[forward-mode {asm | ssm | mac | auto}	**ip multicast forward-mode**
[update-delay-interval *milliseconds***]**	**ip multicast update-delay-interval**
[fast-join {enable | disable}]	**ip multicast fast-join**
[initial-packet-buffer admin-state {enable | disable}]	**ip multicast initial-packet-buffer admin-state**
[initial-packet-buffer max-flow [*num***]]**	**ip multicast initial-packet-buffer max-flow**
[initial-packet-buffer max-packet [*num***]]**	**ip multicast initial-packet-buffer max-packet**
[initial-packet-buffer timeout [*seconds***]**	**ip multicast initial-packet-buffer timeout**
[initial-packet-buffer min-delay [milliseconds]	**ip multicast initial-packet-buffer min-delay**

Examples

```
-> ip multicast profile “IGMPv3 with Zapping”
-> ip multicast profile “IGMPv3 with Zapping” admin-state enable
-> ip multicast profile “IGMPv3 with Zapping” zapping enable version 3
-> ip multicast profile “IGMPv3 with Zapping” fast-join enable proxying enable
-> no ip multicast profile “IGMPv3 with Zapping” proxying
-> no ip multicast profile “IGMPv3 with Zapping”
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

ip multicast apply-profile	Assigns an IPMS configuration profile globally for the switch or to a specific VLAN or service instance.
show ip multicast	Displays the profile assignment for the IPMS instance.
show ip multicast profile	Displays the IPMS profile configuration.

MIB Objects

```
 alaIpmsProfileTable
   alaIpmsProfileAddressType
   alaIpmsProfileName
   alaIpmsProfileIndex
   alaIpmsProfileRowStatus
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigProfileName
```

ip multicast apply-profile

Assigns the name of an existing IPMS configuration profile to the global IPMS instance (all VLANs and services) or to a specific VLAN or Shortest Path Bridging (SPB) service instance. An IPMS configuration profile defines parameter options that are applied to the IPMS instance to which the profile is assigned.

ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] apply-profile** *profile_name*

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] appy-profile**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
profile_name	The name to associate with the IPMS profile.

Defaults

There is a “default” profile that defines a default set of IPMS parameter values that is automatically assigned to an IPMS instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to revert the profile assignment back to the “default” profile.
- Specify a range of VLANs (**vlan 20-25**) or a range of SPB services (**service 10-15**) to apply the specified profile to multiple VLANs or services with one CLI command.
- The specified profile name must already exist in the switch configuration.

Examples

```
-> ip multicast apply-profile “IGMPv3 with Zapping”
-> ip multicast vlan 20 apply-profile “IGMPv3 with Zapping”
-> ip multicast vlan 20-25 apply-profile “IGMPv3 with Zapping”
-> ip multicast service 10 apply-profile “IGMPv3 with Zapping”
-> ip multicast service 10-15 apply-profile “IGMPv3 with Zapping”
-> no ip multicast apply-profile
-> no ip multicast vlan 20 apply-profile
-> no ip multicast vlan 20-15 apply-profile
-> no ip multicast service 10 apply-profile
-> no ip multicast service 10-15 apply-profile
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

ip multicast profile	Defines an IPMS profile that is used to apply a pre-defined IPMS configuration.
show ip multicast	Displays the profile assignment for the IPMS instance.
show ip multicast profile	Displays the IPMS profile configuration.

MIB Objects

```
alaIpmsProfileTable
  alaIpmsProfileAddressType
  alaIpmsProfileName
  alaIpmsProfileIndex
  alaIpmsProfileRowStatus
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigProfileName
```

ipv6 multicast admin-state

Enables or disables IPv6 Multicast Switching and Routing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] admin-state [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] admin-state**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable IPv6 Multicast Switching and Routing.
disable	Disable IPv6 Multicast Switching and Routing.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configuration of an IPv6 multicast routing protocol on an IPv6 interface operationally triggers IP Multicast Switching and Routing functionality on any underlying VLAN or SPB service. This occurs regardless of any explicit IPMS configuration, such as attempting to specifically disable IPMS.
- If there is no IPv6 Multicast routing protocol already running on the switch, then the **ipv6 multicast admin-state** command alone controls IPMS operations.
- Enabling IPMS on individual VLANs or services, as needed, is recommended to conserve switch resources.
- If the IPv6 Multicast Switching and Routing is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.

Note. Globally enabling the IPv6 Multicast Switching and Routing status for the switch only applies to the VLAN domain (does not apply to the service domain). As a result, IPv6 Multicast Switching and Routing must be explicitly enabled or disabled for each SPB service. However, globally disabling IPMS for all SPB services is supported.

- Use the **no** form of this command to restore the IPv6 Multicast Switching and Routing status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ipv6 multicast admin-state enable
-> ipv6 multicast admin-state disable
-> no ipv6 multicast admin-state
-> ipv6 multicast vlan 2 admin-state enable
-> ipv6 multicast vlan 3-5 admin-state disable
-> no ipv6 multicast vlan 2 admin-state
-> no ipv6 multicast vlan 3-5 admin-state
-> ipv6 multicast service 10 admin-state enable
-> ipv6 multicast service 11-15 admin-state disable
-> no ipv6 multicast service 10 admin-state
-> no ipv6 multicast service 11-15 admin-state
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigStatus
```

ipv6 multicast flood-unknown

Enables or disables the flooding of initial unknown multicast traffic for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified. When a traffic flow is first seen on a port. there is a brief period of time where traffic may get dropped before the forwarding information is calculated. When flooding unknown multicast traffic is enabled, no packets are dropped before the forwarding information is available.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] flood-unknown [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] flood-unknown**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32,* or *OmniSwitch 6900-V72.*
enable	Enable flooding of unknown traffic until it is learned.
disable	Disable flooding of unknown traffic.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If this command function is enabled after the system is up and running, the flooding of unknown multicast traffic only applies to new flows.
- On an OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 6900:
  - Configuring the flood unknown status for any VLAN enforces the flood unknown behavior globally across all VLANs. The IPv4 multicast version of this command (**ip multicast flood-unknown**), however, enforces the flood unknown behavior at the per-VLAN level.
  - IPv6 multicast snooping for VLANs does not snoop ff02::/64 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to the excluded IPv6 addresses.
  - When IPv6 multicast snooping is enabled for any service, the flooding of unknown multicast traffic is unconditionally enforced for all snooping services; this is the only supported flood unknown behavior for services.
  - IPv6 multicast snooping for services does not snoop MAC addresses that fall within the range of 01:00:5e:00:00:00/40 and 33:33:00:00:00:00/40 and the traffic is allowed to flood even if the

flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to the excluded MAC addresses.

- On an OmniSwitch 9900, IPv6 multicast snooping for VLANs or services does not snoop ff02::/120 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to these excluded IPv6 addresses.
- Use this command to provide an "open failure" strategy for when hardware resource conflicts or software limits prevent the traffic from being registered in the fast path.
- Use the **no** form of this command to restore the flooding of unknown traffic back to the default value (disabled) on the system.

Examples

```
-> ipv6 multicast flood-unknown enable
-> ipv6 multicast flood-unknown disable
-> no ipv6 multicast flood-unknown
-> ipv6 multicast vlan 100 flood-unknown enable
-> ipv6 multicast vlan 101-105 flood-unknown enable
-> ipv6 multicast vlan 100 flood-unknown disable
-> no ipv6 multicast vlan 100 flood-unknown
-> no ipv6 multicast vlan 101-105 flood-unknown
-> ipv6 multicast service 10 flood-unknown enable
-> ipv6 multicast service 11-15 flood-unknown enable
-> ipv6 multicast service 10 flood-unknown disable
-> no ipv6 multicast service 10 flood-unknown
-> no ipv6 multicast service 11-15 flood-unknown
```

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; **vlan** and **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigFloodUnknown
```

ipv6 multicast version

Sets the default version of the MLD protocol on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] version [***version***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] version**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
version	Default MLD protocol version to run. Valid entries are 1 or 2.

Defaults

parameter	default
version	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the default MLD protocol version on the system and/or the specified VLANs. or SPB services.
- If the default MLD protocol version is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Due to protocol inter-operation requirements, this command specifies only a default version of the MLD protocol to run.
- Use the **no** form of this command to restore the MLD multicast version back to the default value (version 1) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, ipv6 multicast version 0).

Examples

```
-> ipv6 multicast version 2
-> ipv6 multicast version 0
-> no ipv6 multicast version
-> ipv6 multicast vlan 2 version 2
-> ipv6 multicast vlan 3-5 version 2
-> ipv6 multicast vlan 2 version 0
-> no ipv6 multicast vlan 2 version
```

```
-> no ipv6 multicast vlan 3-5 version
-> ipv6 multicast service 2 version 3
-> ipv6 multicast service 3-5 version 3
-> ipv6 multicast service 2 version 0
-> no ipv6 multicast service 2 version
-> no ipv6 multicast service 3-5 version
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigVersion
```

ipv6 multicast port max-group

Configures the maximum group limit learned per port. The limit is applicable on the given port for all VLAN instances or all SPB service instances of the port.

ipv6 multicast {port *chassis/slot/port* **| sap port** *sap_id***} max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

chassis	The chassis identifier.
slot|port	The slot and port number (3/1).
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
num	The maximum MLD group count. Valid range is 0–4294967295.
none	Disables the maximum group limit configuration.
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.A leave is not sent to the router for the replaced group.

Defaults

By default, the max-group limit is set to zero.

parameter	defaults
Action	**none**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If group memberships are already registered on a port/VLAN or SAP port/SPB service instance and the group limit is set to a lower value for the instance, the current group memberships are not removed until they expire. The effect of the new lower group limit value is applied when one of the following occurs to help avoid any undetermined behavior:
  - IP multicast memberships are aged out on a port/VLAN or SAP port/SPB service instance.
  - IP multicast memberships are pruned by a leave or when IP multicast is disabled on the specific VLAN or SPB service or globally disabled for the switch.
- The configuration is allowed even when the IP multicast status is disabled.
- If the *num* and **action** parameters are not specified, then the limit is removed.
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ip multicast sap port 1/1/23:10 max-group 10 action drop, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, "Service Manager Commands," for more information.
- The maximum group configuration on a port will override the VLAN, SPB service, or global configuration.
- MLD zapping must be enabled when the maximum group limit is enabled and the action is dropped.
- The maximum group configuration is applied in the following order of precedence (listed from highest to lowest precedence):
  - Group limit configured for a port or an SPB SAP port.
  - Group limit configured for a specific VLAN or SPB service.
  - Group limit configured for the IPMS profile assigned to a VLAN or SPB service.
  - Group limit configured for a VLAN or SPB service within a specific VRF context.
  - Group limit configured for the IPMS profile assigned to a VLAN or SPB service within a specific VRF context.

Examples

```
-> ipv6 multicast port 1/1/12 max-group 10 action drop
-> ipv6 multicast port 1/1/14 max-group action replace
-> ipv6 multicast port 1/1/14 max-group
-> ipv6 multicast sap port 1/1/23:10 max-group 10 action drop
-> ipv6 multicast sap port 1/1/26:20.200 max-group 20 action replace
-> ipv6 multicast sap port 1/1/16:20.200 max-group
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **sap port** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.
show ipv6 multicast port	Displays the maximum group configuration for VLAN ports or SPB service SAP ports.

MIB Objects

```
alaIpmsIntfTable
   alaIpmsIntfConfigType
   alaIpmsIntfAddressType
   alaIpmsIntfMaxGroupLimit
   alaIpmsIntfMaxGroupExceedAction
```

ipv6 multicast max-group

Configures the maximum group limit learned per port for the specified VLAN, Shortest Path Bridging (SPB) service, or per port on the system if no VLAN or SPB service is specified. The limit is applied to each port that is a member of the given VLAN or SPB service and the specified action is taken when the limit is exceeded.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]** | **service** *service_id***[-***service_id2***]] max-group [***num***] [action {none | drop | replace}]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
num	The maximum MLD group count. Valid range is 0–4294967295.
none	Disables the maximum group limit configuration.
drop	Drops the incoming membership request.
replace	Replaces an existing membership with the incoming membership request.

Defaults

By default, the max-group limit is set to zero.

parameter	defaults
action	**none**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a VLAN or SPB service is not specified, this command configures the global maximum group limit applied to all VLAN ports and SPB Service Access Point (SAP) ports.
- If a VLAN is specified, this command configures the maximum group limit learned per port on a VLAN. The limit is applied to each port that is a member of the given VLAN.
- If an SPB service is specified, this command configures the maximum group limit learned per port on an SPB service. The limit is applied to each port that is a member of the given SPB service.
- Configuring a maximum group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN or port/SPB service instance
- The configuration of a maximum group limit is allowed even when the IP multicast status is disabled.

- If the *num* and **action** parameters are not specified, then the limit is removed.
- The maximum group configuration on a VLAN or SPB service will override the global configuration.
- The maximum group configuration is applied in the following order of precedence (listed from highest to lowest precedence):
  - Group limit configured for a port or an SPB SAP port.
  - Group limit configured for a specific VLAN or SPB service.
  - Group limit configured for the IPMS profile assigned to a VLAN or SPB service.
  - Group limit configured for a VLAN or SPB service within a specific VRF context.
  - Group limit configured for the IPMS profile assigned to a VLAN or SPB service within a specific VRF context.
- MLD zapping must be enabled when the max-group limit is enabled and the action is dropped.

Examples

```
-> ipv6 multicast max-group 10 action drop
-> ipv6 multicast max-group 20 action replace
-> ipv6 multicast max-group
-> ipv6 multicast vlan 10 max-group 10 action drop
-> ipv6 multicast vlan 20 max-group action drop
-> ipv6 multicast vlan 11-15 max-group 10 action replace
-> ipv6 multicast service 5 max-group 10 action drop
-> ipv6 multicast service 20 max-group action drop
-> ipv6 multicast service 10-15 max-group 10 action replace
-> ipv6 multicast service 5 max-group
-> ipv6 multicast service 10-15 max-group
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigMaxGroupLimit
   alaIpmsConfigMaxGroupExceedAction
```

ipv6 multicast static-neighbor

Creates a static MLD neighbor entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

ipv6 multicast static-neighbor vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

ipv6 multicast static-neighbor service *service_id* **sap {port** | **linkagg} {***sap_id***}**

no ipv6 multicast static-neighbor vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ipv6 multicast static-neighbor service *service_id* **sap {port** | **linkagg} {***sap_id***}**

Syntax Definitions

vlan_id	VLAN to include as a static MLD neighbor.
chassis	The chassis identifier.
slot|*port*	The slot and port number to configure as a static MLD neighbor.
agg_id	The link aggregate to configure as a static MLD neighbor.
service_id	SPB service ID to include as a static MLD neighbor. The valid range is 1–32767. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an MLD static neighbor entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an MLD static neighbor entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive all of the MLD traffic *and* IPv6 multicast traffic.
- To create an MLD static neighbor entry on a link aggregate, use the **linkagg** parameter (for example, ipv6 multicast static-neighbor vlan 2 linkagg 7 or ipv6 multicast static-neighbor service 10 sap linkagg 10:100).
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ipv6 multicast static-neighbor service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, "Service Manager Commands," for more information.

Examples

```
-> ipv6 multicast static-neighbor vlan 4 port 1/1
-> no ipv6 multicast static-neighbor vlan 4 port 1/1
-> ipv6 multicast static-neighbor vlan 4 port 7
-> no ipv6 multicast static-neighbor vlan 4 port 7

-> ipv6 multicast static-neighbor service 10 sap port 1/1/2:100
-> no ipv6 multicast static-neighbor service 10 sap port 1/1/2:100
-> ipv6 multicast static-neighbor service 10 sap linkagg 10:100
-> no ipv6 multicast static-neighbor service 10 sap linkagg 10:100
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.
Release 8.4.1; **service** and **sap** parameters added.

Related Commands

show ipv6 multicast neighbor	Displays the MLD neighbor table entries of IPv6 Multicast Switching and Routing.

MIB Objects

```
alaIpmsStaticNeighborTable
   alaIpmsStaticNeighborConfigType
   alaIpmsStaticNeighborAddressType
   alaIpmsStaticNeighborValue
   alaIpmsStaticNeighborIfIndex
   alaIpmsStaticNeighborSubValue
   alaIpmsStaticNeighborRowStatus
```

ipv6 multicast static-querier

Creates a static MLD querier entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

ipv6 multicast static-querier vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

ipv6 multicast static-querier service *service_id* **sap {port** | **linkagg} {***sap_id***}**

no ipv6 multicast static-querier vlan *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ipv6 multicast static-querier service *service_id* **sap {port** | **linkagg} {***sap_id***}**

Syntax Definitions

vlan_id	VLAN to include as a static MLD querier.
chassis	The chassis identifier.
slot|*port*	The slot and port number to configure as a static MLD querier.
agg_id	The link aggregate to configure as a static MLD querier.
service_id	SPB service ID to include as a static MLD querier. The valid range is 1–32767. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an MLD static querier entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an MLD static querier entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive all of the MLD traffic.
- To create an MLD static querier entry on a link aggregate, use the **linkagg** parameter (for example, ipv6 multicast static-querier vlan 2 linkagg 7 or ipv6 multicast static-querier service 10 sap linkagg 10:100).
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ipv6 multicast static-neighbor service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, "Service Manager Commands," for more information.

Examples

```
-> ipv6 multicast static-querier vlan 4 port 1/1
-> no ipv6 multicast static-querier vlan 4 port 1/1
-> ipv6 multicast static-querier vlan 4 port 7
-> no ipv6 multicast static-querier vlan 4 port 7

-> ipv6 multicast static-querier service 10 sap port 1/1/2:100
-> no ipv6 multicast static-querier service 10 sap port 1/1/2:100
-> ipv6 multicast static-querier service 10 sap linkagg 10:100
-> no ipv6 multicast static-querier service 10 sap linkagg 10:100
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.
Release 8.4.1; **service** and **sap** parameters added.

Related Commands

show ipv6 multicast querier	Displays the MLD querier table entries of IPv6 Multicast Switching and Routing.

MIB Objects

```
alaIpmsStaticQuerierTable
   alaIpmsStaticQuerierConfigType
   alaIpmsStaticQuerierAddressType
   alaIpmsStaticQuerierValue
   alaIpmsStaticQuerierIfIndex
   alaIpmsStaticQuerierSubValue
   alaIpmsStaticQuerierRowStatus
```

ipv6 multicast static-group

Creates a static MLD group entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

ipv6 multicast static-group *ipv6_address* **vlan** *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

ipv6 multicast static-group *ipv6_address* **service** *service_id* **sap {port** | **linkagg} {***sap_id***}**

no ipv6 multicast static-group *ipv6_address* **vlan** *vlan_id* **{port** *chassis/slot/port* | **linkagg** *agg_id***}**

no ipv6 multicast static-group *ipv6_address* **service** *service_id* **sap {port** | **linkagg} {***sap_id***}**

Syntax Definitions

ipv6_address	IPv6 multicast group address.
vlan_id	VLAN to include as a static MLD group.
chassis	The chassis identifier.
slot|port	The slot and port number to configure as a static MLD group.
agg_id	The link aggregate to configure as a static MLD group.
service_id	SPB service ID to include as a static MLD group. The valid range is 1–32767. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an MLD static group entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an MLD static group entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive MLD traffic addressed to the specified IP multicast group address.
- To create an MLD static group entry on a link aggregate, use the **linkagg** parameter (for example, ipv6 multicast static-group 225.0.0.1 vlan 2 linkagg 7 or ipv6 multicast static-group 225.0.0.1 service 10 sap linkagg 10:100).
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ipv6 multicast static-querier service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, "Service Manager Commands," for more information.

Examples

```
-> ipv6 multicast static-group ff05::4681 vlan 4 port 1/1
-> no ipv6 multicast static-group ff05::4681 vlan 4 port 1/1
-> ipv6 multicast static-group ff05::4681 vlan 4 port 7
-> no ipv6 multicast static-group ff05::4681 vlan 4 port 7

-> ipv6 multicast static-group 229.10.10.10 service 10 sap port 1/1/2:100
-> no ipv6 multicast static-group 229.10.10.10 service 10 sap port 1/1/2:100
-> ipv6 multicast static-group 225.11.11.11 service 10 sap linkagg 10:100
-> no ipv6 multicast static-group 225.11.11.11 service 10 sap linkagg 10:100
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.
Release 8.4.1; **service** and **sap** parameters added.

Related Commands

show ipv6 multicast group	Displays the MLD group membership table entries of IPv6 Multicast Switching and Routing for the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

MIB Objects

```
alaIpmsStaticMemberTable
   alaIpmsStaticMemberConfigType
   alaIpmsStaticMemberAddressType
   alaIpmsStaticMemberValue
   alaIpmsStaticMemberIfIndex
   alaIpmsStaticMemberSubValue
   alaIpmsStaticMemberGroupAddress
   alaIpmsStaticMemberRowStatus
```

ipv6 multicast query-interval

Sets the MLD query interval on the specified VLAN, Shortest Path Bridging (SPB), or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***] query-interval [***seconds***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***] query-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
seconds	MLD query interval in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	125

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD query interval on the system and/or the specified VLANs or SPB services.
- If the MLD query interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The MLD query interval refers to the time period between MLD query messages.
- Due to protocol inter-operation requirements, this command specifies only a default version of the MLD query interval to use.
- Use the **no** form of this command to restore the MLD query interval back to the default value (125 seconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, **ipv6 multicast query-interval 0**).

Examples

```
-> ipv6 multicast query-interval 100
-> ipv6 multicast query-interval 0
-> no ipv6 multicast query-interval
-> ipv6 multicast vlan 2 query-interval 100
```

```
-> ipv6 multicast vlan 3-5 query-interval 100
-> ipv6 multicast vlan 2 query-interval 0
-> no ipv6 multicast vlan 2 query-interval
-> no ipv6 multicast vlan 3-5 query-interval
-> ipv6 multicast service 2 query-interval 100
-> ipv6 multicast service 3-5 query-interval 100
-> ipv6 multicast service 2 query-interval 0
-> no ipv6 multicast service 2 query-interval
-> no ipv6 multicast service 3-5 query-interval
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQueryInterval
```

ipv6 multicast last-member-query-interval

Sets the MLD last member query interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] last-member-query-interval [***milliseconds***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] last-member-query-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
milliseconds	MLD last member query interval in milliseconds. Valid range is 1–65535.

Defaults

parameter	default
milliseconds	1000

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD last member query interval to use on the system and/or the specified VLANs or SPB services.
- If the MLD last member query interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The MLD last member query interval refers to the time period to reply to an MLD query message sent in response to a leave group message.
- Use the **no** form of this command to restore the MLD last member query interval back to the default value (1000 milliseconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, **ipv6 multicast last-member-query-interval 0**).

Examples

```
-> ipv6 multicast last-member-query-interval 2200
-> ipv6 multicast last-member-query-interval 0
-> no ipv6 multicast last-member-query-interval
```

```
-> ipv6 multicast vlan 4 last-member-query-interval 2200
-> ipv6 multicast vlan 3-5 last-member-query-interval 2200
-> ipv6 multicast vlan 4 last-member-query-interval 0
-> no ipv6 multicast vlan 4 last-member-query-interval
-> no ipv6 multicast vlan 3-5 last-member-query-interval
-> ipv6 multicast service 2 last-member-query-interval 2200
-> ipv6 multicast service 3-5 last-member-query-interval 2200
-> ipv6 multicast service 2 last-member-query-interval 0
-> no ipv6 multicast service 2 last-member-query-interval
-> no ipv6 multicast service 3-5 last-member-query-interval
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigLastMemberQueryInterval
```

ipv6 multicast query-response-interval

Sets the MLD query response interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***] query-response-interval [***milliseconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***] query-response-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
milliseconds	MLD query response interval in milliseconds. Valid range is 1–65535.

Defaults

parameter	default
milliseconds	10000

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD query response interval to use on the system and/or the specified VLANs or SPB services.
- If the MLD query response interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The MLD query response interval refers to the time period to reply to an MLD query message.
- Use the **no** form of this command to restore the MLD query response interval back to the default value (10000 milliseconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, **ipv6 multicast query-response-interval 0**).

Examples

```
-> ipv6 multicast query-response-interval 20000
-> ipv6 multicast query-response-interval 0
-> no ipv6 multicast query-response-interval
-> ipv6 multicast vlan 2 query-response-interval 20000
-> ipv6 multicast vlan 3-5 query-response-interval 20000
-> ipv6 multicast vlan 2 query-response-interval 0
-> no ipv6 multicast vlan 2 query-response-interval
```

```
-> no ipv6 multicast vlan 3-5 query-response-interval
-> ipv6 multicast service 2 query-response-interval 300
-> ipv6 multicast service 3-5 query-response-interval 300
-> ipv6 multicast service 2 query-response-interval 0
-> no ipv6 multicast service 2 query-response-interval
-> no ipv6 multicast service 3-5 query-response-interval
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQueryReponseInterval
```

ipv6 multicast unsolicited-report-interval

Sets the value of the MLD unsolicited report interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] unsolicited-report-interval [***seconds***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] unsolicited-report-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
seconds	MLD unsolicited report interval in seconds. Valid range is 1–65535, where 0 represents the default setting.

Defaults

parameter	default
seconds	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD unsolicited report interval to use on the system and/or the specified VLANs or SPB services.
- If the MLD unsolicited report interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The unsolicited report interval refers to the time period to proxy any changed MLD membership state.
- Use the **no** form of this command to restore the MLD unsolicited report interval back to the default value (1 second) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, **ipv6 multicast unsolicited-report-interval 0**).

Examples

```
-> ipv6 multicast unsolicited-report-interval 20000
-> ipv6 multicast unsolicited-report-interval 0
-> no ipv6 multicast unsolicited-report-interval
-> ipv6 multicast vlan 2 unsolicited-report-interval 20000
```

```
-> ipv6 multicast vlan 3-5 unsolicited-report-interval 20000
-> ipv6 multicast vlan 2 unsolicited-report-interval 0
-> no ipv6 multicast vlan 2 unsolicited-report-interval
-> no ipv6 multicast vlan 3-5 unsolicited-report-interval
-> ipv6 multicast service 2 unsolicited-report-interval 300
-> ipv6 multicast service 3-5 unsolicited-report-interval 300
-> ipv6 multicast service 2 unsolicited-report-interval 0
-> no ipv6 multicast service 2 unsolicited-report-interval
-> no ipv6 multicast service 3-5 unsolicited-report-interval
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigUnsolicitedReportInterval
```

ipv6 multicast router-timeout

Configures the expiry time of IPv6 multicast routers on the specified VLAN, Shortest Path Bridging (SPB) service or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] router-timeout [***seconds***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] router-timeout**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
seconds	MLD router timeout in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	90

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD router timeout on the system and/or the specified VLANs. apply this configuration.
- If the MLD router timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- Use the **no** form of this command to restore the MLD router timeout back to the default value (90 seconds) on the system or the specified VLAN. In addition, specifying a value of 0 with this command also restores the default value (for example, **ipv6 multicast router-timeout 0**).

Examples

```
-> ipv6 multicast router-timeout 100
-> ipv6 multicast router-timeout 0
-> no ipv6 multicast router-timeout
-> ipv6 multicast vlan 2 router-timeout 100
-> ipv6 multicast vlan 3-5 router-timeout 100
-> ipv6 multicast vlan 2 router-timeout 0
-> no ipv6 multicast vlan 2 router-timeout
-> no ipv6 multicast vlan 3-5 router-timeout
-> ipv6 multicast service 2 router-timeout 100
-> ipv6 multicast service 3-5 router-timeout 100
```

```
-> ipv6 multicast service 2 router-timeout 0
-> no ipv6 multicast service 2 router-timeout
-> no ipv6 multicast servicee 3-5 router-timeout
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigRouterTimeout
```

ipv6 multicast source-timeout

Configures the expiry time of IPv6 multicast sources on the specified VLAN, Shortest Path Bridging (SPB) service or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] source-timeout [***seconds***]**

no ip multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] source-timeout**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
seconds	MLD source timeout in seconds. Valid range is 1–65535.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD source timeout on the system and/or the specified VLANs.
- If the MLD source timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- Use the **no** form of this command to restore the MLD source timeout back to the default value (30 seconds) on the system or the specified VLAN. In addition, specifying a value of 0 with this command also restores the default value (for example, **ipv6 multicast source-timeout 0**).

Examples

```
-> ipv6 multicast source-timeout 100
-> ipv6 multicast source-timeout 0
-> no ipv6 multicast source-timeout
-> ipv6 multicast vlan 2 source-timeout 100
-> ipv6 multicast vlan 3-5 source-timeout 100
-> ipv6 multicast vlan 2 source-timeout 0
-> no ipv6 multicast vlan 2 source-timeout
-> no ipv6 multicast vlan 3-5 source-timeout 100
-> ipv6 multicast service 2 source-timeout 100
-> ipv6 multicast service 3-5 source-timeout 100
-> ipv6 multicast service 2 source-timeout 0
```

```
-> no ipv6 multicast service 2 source-timeout
-> no ipv6 multicast service 3-5 source-timeout
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; service parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigSourceTimeout
```

ipv6 multicast querying

Enables or disables MLD querying on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] querying [{enable | disable}] [static-source-ip** *ipv6_address***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] querying [static-source-ip]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
enable	Enable MLD querying.
disable	Disable MLD querying.
ipv6_address	A static source IPv6 address to use for MLD querying. *This parameter is currently not supported.*

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to enable MLD querying on the system and/or specified VLANs.
- If the MLD querying is already enabled/disabled on the system, then the VLAN configuration will override the system's configuration.
- MLD querying refers to requesting the network's MLD group membership information by sending out MLD queries. MLD querying also involves participating in MLD querier election.
- Use the **no** form of this command to restore the MLD querying status to the default value (disabled) on the system or the specified VLAN.

Examples

```
-> ipv6 multicast querying enable
-> ipv6 multicast querying disable
-> no ipv6 multicast querying
-> ipv6 multicast vlan 2 querying enable
-> ipv6 multicast vlan 3-5 querying disable
-> no ipv6 multicast vlan 2 querying
-> no ipv6 multicast vlan 3-5 querying
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1.R02; **static-source-ip** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQuerying
   alaIpmsConfigQueryingStaticSourceAddress
```

ipv6 multicast robustness

Sets the MLD robustness variable on the specified VLAN, Shortest Path Bridging (SPB) service or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] robustness [***robustness***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] robustness**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
robustness	MLD robustness variable. Valid range is 1–7.

Defaults

parameter	default
robustness	2

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD robustness variable on the system and/or the specified VLANs or SPB services.
- If the MLD robustness variable is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Robustness variable allows fine-tuning on the network, where the expected packet loss would be greater.
- Due to protocol inter-operation requirements, this command specifies only a default version of the MLD robustness variable to use.
- Use the **no** form of this command to restore the MLD robustness variable back to the default value (2) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, **ipv6 multicast robustness 0**).

Examples

```
-> ipv6 multicast robustness 3
-> ipv6 multicast robustness 0
-> no ipv6 multicast robustness
-> ipv6 multicast vlan 2 robustness 3
```

```
-> ipv6 multicast vlan 3-5 robustness 3
-> ipv6 multicast vlan 2 robustness 0
-> no ipv6 multicast vlan 2 robustness
-> no ipv6 multicast vlan 3-5 robustness
-> ipv6 multicast service 2 robustness 3
-> ipv6 multicast service 3-5 robustness 3
-> ipv6 multicast service 2 robustness 0
-> ipv6 multicast service 2 robustness
-> no ipv6 multicast service 3-5 robustness
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigRobustness
```

ipv6 multicast spoofing

Enables or disables MLD spoofing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] spoofing {enable | disable}**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***] spoofing**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable MLD spoofing.
disable	Disable MLD spoofing.

Defaults

parameter	defaults
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the MLD spoofing is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- MLD spoofing refers to replacing a client's MAC and IPv6 address with the system's MAC and IPv6 address when proxying aggregated MLD group membership information.
- By default, the source IPv6 address is not specified for spoofing; the system determines these addresses automatically. Optionally configure a static source IPv6 address to overcome the need for an IPv6 interface. If configured, the static source IPv6 is always used for spoofing, regardless of the IPv6 interface address or administrative state.
- Use the **no** form of this command to remove an MLD spoofing configuration and return the specified VLAN, SPB service, or system to the default behavior.

Examples

```
-> ipv6 multicast spoofing enable
-> ipv6 multicast spoofing disable
-> no ipv6 multicast spoofing
-> ipv6 multicast vlan 2 spoofing enable
```

```
-> ipv6 multicast vlan 3-5 spoofing disable
-> no ipv6 multicast vlan 2 spoofing
-> no ipv6 multicast vlan 3-5 spoofing
-> ipv6 multicast service 2 spoofing enable
-> ipv6 multicast service 3-5 spoofing disable
-> no ipv6 multicast service 2 spoofing
-> no ipv6 multicast service 3-5 spoofing
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigSpoofing
```

ipv6 multicast spoofing static-source-ip

Enables or disables MLD static spoofing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] spoofing static-source-ip** *ipv6_address*

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] spoofing static-source-ip**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
ipv6_address	A static source IPv6 address to use for spoofing.

Defaults

parameter	defaults
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a static source IP address.
- MLD spoofing refers to replacing a client's MAC and IPv6 address with the system's MAC and IPv6 address when proxying aggregated MLD group membership information.
- By default, the source IPv6 address is not specified for spoofing; the system determines these addresses automatically. Optionally configure a static source IPv6 address to overcome the need for an IPv6 interface. If configured, the static source IPv6 is always used for spoofing, regardless of the IPv6 interface address or administrative state.

Examples

```
-> ipv6 multicast spoofing static-source-ip 3333::1
-> no ipv6 ip multicast spoofing static-source-ip
-> ipv6 multicast vlan 2 spoofing static-source-ip 3333::1
-> ipv6 multicast vlan 3-5 spoofing static-source-ip 3333::1
-> no ipv6 ip multicast vlan 2 spoofing static-source-ip
-> no ipv6 multicast vlan 3-5 spoofing static-source-ip
-> ipv6 multicast service 2 spoofing static-source-ip 3333::1
-> no ipv6 multicast service 2 spoofing static-source-ip
-> ipv6 multicast service 3-5 spoofing static-source-ip 3333::1
```

```
-> no ipv6 multicast service 3-5 spoofing static-source-ip
```

Release History

Release 8.3.1.R02; command was added.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigSpoofing
  alaIpmsConfigSpoofingStaticSourceAddress
```

ipv6 multicast zapping

Enables or disables MLD zapping on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] zapping [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] zapping**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable MLD zapping.
disable	Disable MLD zapping.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the MLD zapping is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- MLD zapping refers to processing membership and source filter removals immediately and not waiting for the protocol's specified time period. This mode facilitates IP TV applications looking for quick changes between IP multicast groups.
- Use the **no** form of this command to restore the MLD zapping status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ipv6 multicast zapping enable
-> ipv6 multicast zapping disable
-> no ipv6 multicast zapping
-> ipv6 multicast vlan 2 zapping enable
-> ipv6 multicast vlan 3-5 zapping disable
-> no ipv6 multicast vlan 2 zapping
-> no ipv6 multicast vlan 3-5 zapping
-> ipv6 multicast service 2 zapping enable
```

```
-> ipv6 multicast service 3-5 zapping disable
-> no ipv6 multicast service 2 zapping
-> no ip multicast service 3-5 zapping
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigZapping
```

ipv6 multicast querier-forwarding

Enables or disables MLD querier forwarding on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] querier-forwarding [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] querier-forwarding**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable MLD querier forwarding.
disable	Disable MLD querier forwarding.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the MLD querier forwarding is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- MLD querier forwarding refers to promoting detected MLD queriers to receive all IP multicast data traffic.
- Use the **no** form of this command to restore the MLD querier forwarding status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ipv6 multicast querier-forwarding enable
-> ipv6 multicast querier-forwarding disable
-> no ipv6 multicast querier-forwarding
-> ipv6 multicast vlan 2 querier-forwarding enable
-> ipv6 multicast vlan 3-5 querier-forwarding disable
-> no ipv6 multicast vlan 2 querier-forwarding
-> no ipv6 multicast vlan 3-5 querier-forwarding
-> ipv6 multicast service 2 querier-forwarding enable
```

```
-> ipv6 multicast service 3-5 querier-forwarding disable
-> no ipv6 multicast service 2 querier-forwarding
-> no ip multicast service 3-5 querier-forwarding
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQuerierForwarding
```

ipv6 multicast proxying

Enables or disables MLD proxying on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] proxying [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] proxying**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable MLD proxying.
disable	Disable MLD proxying.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the MLD proxying is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- MLD proxying refers to processing membership information on behalf of client systems and reporting membership on their behalf.
- Proxy reported MLD packets are sent using the source MAC address of the proxying switch. Unless the spoofing feature is used, proxy reported MLD packets will be sent using "::" for the IPv6 source address.
- Use the **no** form of this command to restore the MLD proxying status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ipv6 multicast proxying enable
-> ipv6 multicast proxying disable
-> no ipv6 multicast proxying
-> ipv6 multicast vlan 2 proxying enable
-> ipv6 multicast vlan 3-5 proxying disable
-> no ipv6 multicast vlan 2 proxying
-> no ipv6 multicast vlan 3-5 proxying
-> ipv6 multicast service 2 proxying enable
-> ipv6 multicast service 3-5 proxying disable
-> no ipv6 multicast service 2 proxying
-> no ip multicast service 3-5 proxying
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigProxying
```

ipv6 multicast helper-address

Specifies the destination IPv6 address of a relay host where MLD host Reports and Leave messages are sent.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] helper-address [***ipv6_address***]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] helper-address**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
ipv6_address	The IPv6 address of the relay host.

Defaults

By default, no destination IPv6 address is set.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- After the destination IPv6 address is specified, the IPMS reporting feature is enabled.
- An operational IPv6 interface is required for the receiving LAN before any MLD Reports and Leave messages can be relayed.
- Configuring a destination IPv6 helper address is supported only in the VLAN domain; the service domain is not supported.
- Use the **no** form of this command to restore the IPMS reporting feature back to the default value (no IPv6 helper address) on the system. When there is no IPv6 helper address set, the IPMS reporting feature is disabled.

Examples

```
-> ipv6 multicast helper-address 3333::2
-> no ipv6 multicast helper-address
-> ipv6 multicast vlan 2 helper-address 3333::2
-> ipv6 multicast vlan 3-5 helper-address 3333::2
-> no ipv6 multicast vlan 2 helper-address
-> no ipv6 multicast vlan 3-5 helper-address
```

Release History

Release 8.4.1; command was introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigHelperAddress
```

ipv6 multicast zero-based-query

Configures the use of an all-zero source IPv6 address for MLD query packets when a non-querier is querying the membership of a port. This value is set for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] zero-based-query [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] zero-based-query**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
enable	Enable MLD zero-based querying.
disable	Disable MLD zero-based querying.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The MLD zero-based query status set for a specific VLAN or SPB service overrides the zero-based query status set for the system.
- Use the **no** form of this command to restore the MLD zero-based query status back to the default value (enabled) on the system, the specified VLAN, or the specified SPB service.

Examples

```
-> ipv6 multicast zero-based-query enable
-> ipv6 multicast zero-based-query disable
-> no ipv6 multicast zero-based-query
-> ipv6 multicast vlan 2 zero-based-query enable
-> ipv6 multicast vlan 3-5 zero-based-query disable
-> no ipv6 multicast vlan 2 zero-based-query
-> no ipv6 multicast vlan 3-5 zero-based-query
-> ipv6 multicast service 10 zero-based-query enable
-> ipv6 multicast service 11-15 zero-based-query disable
-> no ipv6 multicast service 10 zero-based-query
```

```
-> no ipv6 multicast service 11-15 zero-based-query disable
```

Release History

Release 8.3.1; command introduced.
Release 8.4.1; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigZeroBasedQuery
```

ipv6 multicast forward-mode

Configures the Layer 2 forwarding mode for IPv6 Multicast Switching (does not apply to IPv6 Multicast Routing).The forwarding mode is set for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] forward-mode {asm | ssm | mac | auto}**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] forward-mode**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
asm	Sets the IPMSv6 forwarding mode to ASM (the bridge lookup is based on the packet group destination IPv6 address). *This parameter is supported only in the VLAN domain; service domain is not supported.*
ssm	Sets the IPMSv6 forwarding mode to SSM (the bridge lookup is based on the packet source IPv6 as well as the group destination IPv6). *This parameter is supported only in the VLAN domain; service domain is not supported.*
mac	Sets the IPMSv6 forwarding mode to MAC address (the bridge lookup is based on the MAC destination address).
auto	Automatically determines the IPMSv6 forwarding mode based on the current MLD protocol version and the existing protocol state.

Defaults

By default, the forwarding mode is set to automatic.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The forwarding mode set for a specific VLAN or SPB service overrides the forwarding mode set for the system.
- If multicast routing is enabled on a VLAN, the following conditions apply:
  - On the OmniSwitch 9900, the bridging mode is independent of the routing mode. As a result, ASM bridging is allowed in a VLAN that has SSM routing configured or SSM bridging is allowed in a VLAN that has ASM routing configured.
  - Multicast routing is not supported on the OmniSwitch 6560.
  - On all other OmniSwitch platforms, the routing configuration overrides the forwarding mode setting

and determines the forwarding mode based on the group mappings. For example, BIDIR flows will use ASM while DVMRP flows and all other PIM modes will use SSM.

- Use the **no** form of this command to restore the Layer 2 forwarding mode back to the default value (automatic) on the system, the specified VLAN or SPB service.

Examples

```
-> ipv6 multicast forward-mode auto
-> ipv6 multicast forward-mode asm
-> ipv6 multicast forward-mode ssm
-> ipv6 multicast forward-mode mac
-> no ipv6 multicast forward-mode
-> ipv6 multicast vlan 100 forward-mode auto
-> ipv6 multicast vlan 101-104 forward-mode asm
-> ipv6 multicast vlan 100 forward-mode ssm
-> ipv6 multicast vlan 101-104 forward-mode mac
-> no ipv6 multicast vlan 100 forward-mode
-> no ipv6 multicast vlan 101-104 forward-mode
-> ipv6 multicast service 10 forward-mode mac
-> ipv6 multicast service 11-15 forward-mode mac
-> no ipv6 multicast service 10 forward-mode
-> no ipv6 multicast service 11-15 forward-mode
```

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.
show ipv6 multicast bridge	Displays IPv6 multicast bridge table entries.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigForwardMode
```

ipv6 multicast update-delay-interval

Sets the amount of time to delay IPv6 multicast forwarding updates on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] update-delay-interval** *milliseconds*

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] update-delay-interval**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
milliseconds	The number of milliseconds to defer forwarding updates. Valid range is 0–10000.

Defaults

By default, the forwarding update delay interval is set to zero.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the forwarding update delay is set to zero, forwarding updates are processed immediately with minimal latency. Configuring a forwarding update delay value can limit the effects of persistent churn on the system.
- If the forwarding update delay interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Use the **no** form of this command to restore the forwarding update delay interval back to the default value (zero) on the system or the specified VLAN or SPB service.

Examples

```
-> ipv6 multicast update-delay-interval 10
-> no ipv6 multicast update-delay-interval
-> ipv6 multicast vlan 100 update-delay-interval 20
-> ipv6 multicast vlan 101-105 update-delay-interval 20
-> no ipv6 multicast vlan 100 update-delay-interval 20
-> no iv6p multicast vlan 101-105 update-delay-interval
-> ipv6 multicast service 20 update-delay-interval 20
-> ipv6 multicast service 21-25 update-delay-interval 20
-> no ipv6 multicast service 20 update-delay-interval
-> no ipv6 multicast service 21-25 update-delay-interval
```

Release History

Release 8.3.1; command was introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigUpdateDelayInterval
```

ipv6 multicast fast-join

Configures whether or not IPv6 Multicast Switching will automatically create the forwarding entries in hardware as soon as the MLD memberships are learned on the specified VLAN, Shortest Path Bridging (SPB) service or globally if no VLAN or SPB service is specified.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] fast-join [enable | disable]**

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] fast-join**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs. *This parameter is supported only on the OmniSwitch 9900.*
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6900-C32 or OmniSwitch 6900-V72.*
enable	Enable the MLD fast join functionality.
disable	Disable the MLD fast join functionality.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command applies only to IPv6 Multicast Switching. If IPv6 Multicast Routing is enabled, then the routing configuration will override the fast join setting.
- When the IPv6 Multicast Switching fast join functionality is enabled, convergence of multicast traffic may occur faster because the forwarding entries are already created before the actual multicast traffic is received.
- When the IPv6 Multicast Switching fast join functionality is disabled (the default), forwarding entries are not created in the hardware until the multicast traffic reaches the switch.
- If the IPv6 Multicast Switching fast join is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Use the **no** form of this command to restore the IPv6 Multicast Switching fast join setting back to the default value (disabled) on the system or the specified VLAN or SPB service.

Examples

```
-> ipv6 multicast fast-join enable
-> ipv6 multicast fast-join disable
-> no ipv6 multicast fast-join
-> ip multicast service 10 fast-join enable
-> ip multicast service 11-15 fast-join disable
-> no ip multicast service 10 fast-join
-> no ip multicast service 11-15 fast-join
```

Release History

Release 8.3.1.R02; command introduced.
Release 8.4.1.R02; **vlan** and **service** parameters added.

Related Commands

show ip multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigFastJoin
```

ipv6 multicast host-list

Configures a list of host IP addresses that is used for IP multicast group maps and SSM maps.

ipv6 multicast host-list *host_list_name ipv6_address* **[***ipv6_address***]**

no ipv6 multicast host-list *host_list_name* **[***ipv6_address***]**

Syntax Definitions

host_list_name	A name to assign to the host list (up to 20 characters).
ipv6_address	The IPv6 address to add to the host list. Multiple IPv6 addresses can be entered on the same command line.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Use the **no** form of this command to remove an IPv6 address from the list or remove the entire list from the switch configuration.
- When the entire list is removed, any configuration associated with the list is also removed.

Examples

```
-> ipv6 multicast host-list group-map1 4444::2
-> ipv6 multicast host-list ssm-map1 4444::3
-> ipv6 multicast host-list ssm-map2 3333::2 3333::3 3333::4
-> no ipv6 multicast host-list ssm-map2 3333::3
-> no ipv6 multicast host-list group-map1
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ipv6 multicast host-list	Displays the IPv6 multicast host address list configuration.

MIB Objects

```
alaIpmsHostListTable
   alaIpmsHostListName
   alaIpmsHostListAddressType
   alaIpmsHostListAddress
```

ipv6 multicast ssm-map

Configures the translation of Any Source Multicast (ASM) group memberships into Source Specific Multicast (SSM) group memberships on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vlan_id***] ssm-map {***group_address***[***/prefixLen***]** *host_list_name* | **admin-state {enable | disable}}**

no ipv6 multicast ssm-map *group_address***[***/prefixLen***]**

Syntax Definitions

vlan_id	VLAN on which to apply the mapping configuration.
*group_address***[***/prefixLen***]**	The multicast group address/prefix length to map to the host list. If no prefix length is specified, then the a default length of 128 is used.
host_list_name	The name of a host list to use for SSM mapping.
enable	Enables the SSM mapping.
disable	Disables the SSM mapping.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Use the **no** form of this command to remove the SSM mapping configuration.
- If an SSM mapping is already enabled on the system, then the VLAN configuration will override the system's configuration.

Examples

```
-> ipv6 multicast ssm-map ff05::5 hostList1
-> ipv6 multicast ssm-map admin-state enable
-> ipv6 multicast vlan 200 ssm-map ff05::6 hostList2
-> ipv6 multicast vlan 200 ssm-map admin-state enable
-> no ipv6 multicast ssm-map ff05::5
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ipv6 multicast ssm-map	Displays the SSM mapping configuration.
show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters, such as the global SSM mapping setting.

MIB Objects

```
alaIpmsSsmMapTable
   alaIpmsSsmMapConfigType
   alaIpmsSsmMapConfigAddressType
   alaIpmsSsmMapConfigValue
   alaIpmsSsmMapGroupAddress
   alaIpmsSsmMapGroupPrefixLength
   alaIpmsSsmMapSourceListName
```

ipv6 multicast initial-packet-buffer admin-state

Enables or disables initial packet buffering for IPv6 multicast flows on the specified VLAN or globally on the switch.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer admin-state {enable | disable}**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
enable	Enable the initial packet buffering globally on the switch for IPv6 multicast flow.
disable	Disable the initial packet buffering globally on the switch for IPv6 multicast flow.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- When enabled, the following configuration is used for initial packet buffering on new multicast flows:
  - The maximum number of initial packets buffered per IPv6 multicast flow. Use the **ipv6 multicast initial-packet-buffer max-packet** command to set this value.
  - The maximum number of IPv6 multicast flows that can be buffered. Use the **ipv6 multicast initial-packet-buffer max-flow** command to set this value.
  - The maximum amount of time buffered packets are held if they are not sent out. Use the **ipv6 multicast initial-packet-buffer timeout** command to set this value.
  - The minimum amount of time packets are held before delivery begins. Use the **ipv6 multicast initial-packet-buffer min-delay** command to set this value.
- Configuring the status for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ipv6 multicast initial-packet-buffer admin-state disable
-> ipv6 multicast initial-packet-buffer admin-state enable
-> ipv6 multicast vlan 2 initial-packet-buffer admin-state enable
-> ipv6 multicast vlan 3-5 initial-packet-buffer admin-state enable
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

show ipv6 multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBuffer
```

ipv6 multicast initial-packet-buffer max-packet

Configures the maximum number of initial packets buffered per IPv6 multicast flow on the specified VLAN or globally on the switch.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer max-packet [***num***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
num	The maximum number of packets allowed to buffer per IPv6 multicast flow. Valid range is 1 to 10.

Defaults

parameter	default
num	4

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ipv6 multicast initial-packet-buffer max-packet 4
-> ipv6 multicast vlan 2 initial-packet-buffer max-packet 10
-> ipv6 multicast vlan 3-5 initial-packet-buffer max-packet 10
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

ipv6 multicast initial-packet-buffer admin-state	Enables or disables the initial packet buffering feature globally on the switch for IPv6 multicast flows.
show ipv6 multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferMaxPacket
```

ipv6 multicast initial-packet-buffer max-flow

Configures the maximum number of IPv6 multicast flows that can be buffered on the specified VLAN or globally on the switch.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer max-flow [***num***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
num	The maximum number of IPv6 multicast flows allowed for initial packet buffering. Valid range is 1 to 32.

Defaults

parameter	default
num	32

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ipv6 multicast initial-packet-buffer max-flow 32
-> ipv6 multicast vlan 2 initial-packet-buffer max-flow 32
-> ipv6 multicast vlan 3-5 initial-packet-buffer max-flow 32
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

ipv6 multicast initial-packet-buffer admin-state	Enables or disables the initial packet buffering feature globally on the switch for IPv6 multicast flows.
show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferMaxFlow
```

ipv6 multicast initial-packet-buffer timeout

Configures the timeout value for the buffered IPv6 initial multicast packets on the specified VLAN or globally on the switch.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer timeout [***seconds***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
seconds	The timeout value for the initial buffered IPv6 multicast packets in seconds. Valid range is 1 to 10.

Defaults

parameter	default
seconds	10

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- If the buffered multicast packet is not sent out before the timeout, then the buffered packets will be removed from IPMS system.
- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ipv6 multicast initial-packet-buffer timeout 2
-> ipv6 multicast vlan 2 initial-packet-buffer timeout 5
-> ipv6 multicast vlan 3-5 initial-packet-buffer timeout t
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

ipv6 multicast initial-packet-buffer admin-state	Enables or disables the initial packet buffering feature globally on the switch for IPv6 multicast flows.
show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferTimeout
```

ipv6 multicast initial-packet-buffer min-delay

Configures the minimum delay to program the multicast replication index for IPv6 multicast flows buffered for initial packet on the specified VLAN or globally on the switch.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***]] initial-packet-buffer min-delay [***milliseconds***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
milliseconds	The minimum delay value to program the multicast replication index for IPv6 multicast flows buffered for initial packet. Valid range is 0 to 1000.

Defaults

parameter	default
milliseconds	0

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

Note. This command configures a timer to delay the programming of multicast replication index in hardware which might increase the number of multicast packets lost during the learning phase.

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

```
-> ipv6 multicast initial-packet-buffer min-delay 200
-> ipv6 multicast vlan 2 initial-packet-buffer min-delay 200
-> ipv6 multicast vlan 3-5 initial-packet-buffer min-delay 200
```

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

Related Commands

ipv6 multicast initial-packet-buffer admin-state	Enables or disables the initial packet buffering feature globally on the switch for IPv6 multicast flows.
show ip multicast	Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferMinDelay
```

ipv6 multicast display-interface-names

Sets the display output of the **show** commands listed below.When enabled, the display outputs for these commands will show the IPv6 interface name for each VLAN associated with the IPv6 multicast table entry.

ipv6 multicast display-interface-names

no ipv6 multicast display-interface-names

Syntax Definitions

N/A

Defaults

By default, this function is disabled. The display format is set to include the VLANs that are associated with the IPv6 multicast source and forward flows.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to revert back to displaying the VLAN name.
- If there are any VLANs that are not configured with an IPv6 interface or the IPv6 interface is disabled, the output display will still include the VLAN when this function is enabled.
- This command may be helpful when reviewing output from multicast snooping commands and comparing state in multicast routing, which only interacts with IPv6 interfaces.
- Enabling the display interface names option applies to the following **show** commands:

  show ipv6 multicast forward
  show ipv6 multicast neighbor
  show ipv6 multicast querier
  show ipv6 multicast group
  show ipv6 multicast source
  show ipv6 multicast tunnel

- The command examples provided display the **show ipv6 multicast source** output after the display interface name function is turned on (enabled) and off (disabled).

Examples

```
-> ipv6 multicast display-interface-name

-> show ipv6 multicast source

Total 4 Sources

                                      Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN/Service
---------------+---------------+---------------+--------------
ff05::5         4444::2         ::              VL-21
ff05::6         4444::2         ::              VL-21
ff06::1         ::              ::              VL-20
ff06::1         ::              ::              VL-20

-> no ip multicast display-interface-name

-> show ipv6 multicast source

Total 4 Sources

                                      Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN/Service
---------------+---------------+---------------+--------------
ff05::5         4444::2         ::              vlan 21
ff05::6         4444::2         ::              vlan 21
ff06::1         ::              ::              vlan 20
ff06::1         ::              ::              vlan 20
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ipv6 multicast source	Displays the IPv6 Multicast Switching and Routing source table entries.
show ipv6 multicast forward	Displays the IPv6 Multicast Switching and Routing forwarding table entries.

MIB Objects

```
alaIpmsGlobalConfigTable
   alaIpmsGlobalConfigAddressType
   alaIpmsGlobalConfigDisplayInterfaceNames
```

ipv6 multicast inherit-default-vrf-config

Configures whether or not the global IPMSv6 configuration defined in the default VRF instance is applied to all VRF instances.

ipv6 multicast inherit-default-vrf-config

no ipv6 multicast inherit-default-vrf-config

Syntax Definitions

N/A

Defaults

By default, the global IPMSv6 configuration defined in the default VRF instance is applied to all VRF instances on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable this function. When disabled, the global IPMSv6 configuration defined in the default VRF instance is not applied to all other VRF instances on the switch.
- When enabled, additional VRF instances will inherit the global IPMSv6 configuration defined in the default VRF instance.
- A global IPMSv6 configuration defined for a specific non-default VRF instance takes precedence over the global IPMSv6 configuration defined for the default VRF.

Examples

```
-> ipv6 multicast inherit-default-vrf-config
-> no ipv6 multicast inherit-default-vrf-config
```

Release History

Release 8.3.1; command introduced.

Related Commands

show ipv6 multicast	Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

```
alaIpmsGlobalConfigTable
   alaIpmsGlobalConfigAddressType
   alaIpmsGlobalConfigInheritDefaultVrfConfig
```

ipv6 multicast profile

Defines an IPMS profile that is used to apply a pre-defined configuration to the global IPMS instance (all VLAN and service instances) or to a specific VLAN or service instance. Using a configuration profile to configure IPMS functionality avoids having to configure each IPMS parameter with a separate CLI command.

This section describes the base command (**ipv6 multicast profile**) along with optional command keywords that are used to configure IPMS parameter values that are applied when the profile is assigned to an IPMS instance. Optional keywords are listed separately but can be entered in combination on the same command line. Use the **no** form for the keywords to change a specific parameter value for the profile.

There is a "default" profile that defines a default set of IPMS parameter values that is automatically assigned to an IPMS instance. The default profile cannot be deleted, but the profile parameter values are configurable through this command.

ipv6 multicast profile *profile_name*
[admin-state {enable | disable}]
[flood-unknown {enable | disable}]
[version *version***]**
[robustness *robustness***]**
[querying {enable | disable}]
[query-interval [*seconds***]]**
[query-response-interval [*milliseconds***]]**
[last-member-query-interval [*milliseconds***]]**
[unsolicited-report-interval [*seconds***]]**
[proxying {enable | disable}]
[spoofing {enable | disable}]
[spoofing static-source-ip *ipv6_address***]**
[zapping {enable | disable}]
[querier-forwarding {enable | disable}]
[router-timeout [*seconds***]]**
[source-timeout [*seconds***]]**
[max-group [*num***] [action {none | drop | replace}]]**
[helper-address [*ipv6_address***]]**
[zero-based-query {enable | disable}]
[forward-mode {asm | ssm | mac | auto}
[update-delay-interval *milliseconds***]**
[fast-join {enable | disable}]
[initial-packet-buffer admin-state {enable | disable}]
[initial-packet-buffer max-flow [*num***]]**
[initial-packet-buffer max-packet [*num***]]**
[initial-packet-buffer timeout [*seconds***]**
[initial-packet-buffer min-delay [*milliseconds***]**

no ipv6 multicast profile *profile_name* **[admin-state | flood-unknown | version | robustness | ...]**

Syntax Definitions

profile_name The name to associate with the IPMS profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IPMS profile from the switch configuration.
- To change the value of a specific profile parameter, specify the parameter keyword with this command. For example, **no ipv6 multicast profile ipms-1 admin-state**, **ipv6 multicast profile ipms-1 query-interval 100**, or **ipv6 multicast profile ipms-1 querying enable**. The new parameter values are applied to all IPMS instances to which the profile is assigned.
- The profile name must already exist in the switch configuration before parameter values can be modified. Use this command to create the profile first, then configure the profile parameter values.
- For more information about specific profile parameter values, refer to the following explicit IPMS configuration commands for each profile parameter:

Port Template Parameter	Explicit Port Configuration Command
[admin-state {enable | disable}]	**ipv6 multicast admin-state**
[flood-unknown {enable | disable}]	**ipv6 multicast flood-unknown**
[version *version***]**	**ipv6 multicast version**
[robustness *robustness***]**	**ipv6 multicast robustness**
[querying {enable | disable}]	**ipv6 multicast querying**
[query-interval [*seconds***]]**	**ipv6 multicast query-interval**
[query-response-interval [*milliseconds***]]**	**ipv6 multicast query-response-interval**
[last-member-query-interval [*milliseconds***]]**	**ipv6 multicast last-member-query-interval**
[unsolicited-report-interval [*seconds***]]**	**ipv6 multicast unsolicited-report-interval**
[proxying {enable | disable}]	**ipv6 multicast proxying**
[spoofing {enable | disable}]	**ipv6 multicast spoofing**
[spoofing static-source-ip *ipv6_address***]**	**ipv6 multicast spoofing static-source-ip**
[zapping {enable | disable}]	**ipv6 multicast zapping**
[querier-forwarding {enable | disable}]	**ipv6 multicast querier-forwarding**
[router-timeout [*seconds***]]**	**ipv6 multicast router-timeout**
[source-timeout [*seconds***]]**	**ipv6 multicast source-timeout**
[max-group [*num***] [action {none | drop | replace}]]**	**ipv6 multicast max-group**

Port Template Parameter	Explicit Port Configuration Command
[helper-address [*ipv6_address***]]**	**ipv6 multicast helper-address**
[zero-based-query {enable | disable}]	**ipv6 multicast zero-based-query**
[forward-mode {asm | ssm | mac | auto}	**ipv6 multicast forward-mode**
[update-delay-interval *milliseconds***]**	**ipv6 multicast update-delay-interval**
[fast-join {enable | disable}]	**ipv6 multicast fast-join**
[initial-packet-buffer admin-state {enable | disable}]	**ipv6 multicast initial-packet-buffer admin-state**
[initial-packet-buffer max-flow [*num***]]**	**ipv6 multicast initial-packet-buffer max-flow**
[initial-packet-buffer max-packet [*num***]]**	**ipv6 multicast initial-packet-buffer max-packet**
[initial-packet-buffer timeout [*seconds***]**	**ipv6 multicast initial-packet-buffer timeout**
[initial-packet-buffer min-delay [*milliseconds***]**	**ipv6 multicast initial-packet-buffer min-delay**

Examples

```
-> ipv6 multicast profile “MLDv2 with Zapping”
-> ipv6 multicast profile “MLDv2 with Zapping” admin-state enable
-> ipv6 multicast profile “MLDv2 with Zapping” zapping enable version 2
-> ipv6 multicast profile “MLDv2 with Zapping” fast-join enable proxying enable
-> no ipv6 multicast profile “MLDv2 with Zapping” proxying
-> no ipv6 multicast profile “MLDv2 with Zapping”
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

ipv6 multicast apply-profile	Assigns an IPMS configuration profile globally for the switch or to a specific VLAN or service instance.
show ipv6 multicast	Displays the profile assignment for the IPMS instance.
show ipv6 multicast profile	Displays the IPMS profile configuration.

MIB Objects

```
 alaIpmsProfileTable
   alaIpmsProfileAddressType
   alaIpmsProfileName
   alaIpmsProfileIndex
   alaIpmsProfileRowStatus
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigProfileName
```

ipv6 multicast apply-profile

Assigns the name of an existing IPMS configuration profile to the global IPMS instance (all VLANs and services) or to a specific VLAN or Shortest Path Bridging (SPB) service instance. An IPMS configuration profile defines parameter options that are applied to the IPMS instance to which the profile is assigned.

ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] apply-profile** *profile_name*

no ipv6 multicast [vlan *vlan_id***[-***vlan_id2***] | service** *service_id***[-***service_id2***]] appy-profile**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
*service_id***[-***service_id2***]**	SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
profile_name	The name to associate with the IPMS profile.

Defaults

There is a “default” profile that defines a default set of IPMS parameter values that is automatically assigned to an IPMS instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to revert the profile assignment back to the “default” profile.
- Specify a range of VLANs (**vlan 20-25**) or a range of SPB services (**service 10-15**) to apply the specified profile to multiple VLANs or services with one CLI command.
- The specified profile name must already exist in the switch configuration.

Examples

```
-> ipv6 multicast apply-profile “MLDv2 with Zapping”
-> ipv6 multicast vlan 20 apply-profile “MLDv2 with Zapping”
-> ipv6 multicast vlan 20-25 apply-profile “MLDv2 with Zapping”
-> ipv6 multicast service 10 apply-profile “MLDv2 with Zapping”
-> ipv6 multicast service 10-15 apply-profile “MLDv2 with Zapping”
-> no ipv6 multicast apply-profile
-> no ipv6 multicast vlan 20 apply-profile
-> no ipv6 multicast vlan 20-15 apply-profile
-> no ipv6 multicast service 10 apply-profile
-> no ipv6 multicast service 10-15 apply-profile
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

ipv6 multicast profile	Defines an IPMS profile that is used to apply a pre-defined IPMS configuration.
show ipv6 multicast	Displays the profile assignment for the IPMS instance.
show ipv6 multicast profile	Displays the IPMS profile configuration.

MIB Objects

```
alaIpmsProfileTable
  alaIpmsProfileAddressType
  alaIpmsProfileName
  alaIpmsProfileIndex
  alaIpmsProfileRowStatus
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigProfileName
```

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

show ip multicast [vlan *vlan_id* **| service** *service_id***]**

Syntax Definitions

vlan_id	VLAN ID number (1–4094).
service_id	SPB service ID number (1–32767). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

By default the status and general configuration parameters for the system are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify a VLAN ID to display the configuration information for a specific VLAN.
- Specify an SPB service ID to display the configuration information for a specific SPB service.

Examples

```
-> show ip multicast

Profile                                          = default,
Status                                           = disabled,
Flood Unknown                                    = disabled,
Version                                          = 2,
Robustness                                       = 2,
Querying                                         = disabled,
Query Interval (seconds)                         = 125,
Query Response Interval (tenths of seconds)      = 100,
Last Member Query Interval (tenths of seconds)   = 10,
Unsolicited Report Interval (seconds)            = 1,
Proxying                                         = disabled,
Spoofing                                         = disabled,
Zapping                                          = disabled,
Querier Forwarding                               = disabled,
Router Timeout (seconds)                         = 90,
Source Timeout (seconds)                         = 30,
Max-group                                        = 0,
Max-group action                                 = none,
Helper-address                                   = 0.0.0.0,
Static Querier Address                           = 0.0.0.0,
Static Spoofer Address                           = 0.0.0.0,
```

```
Zero-based Query                                = enabled,
Forward Mode                                    = auto,
Update Delay Interval (milliseconds)            = 0,
SSM Mapping                                     = disabled,
Fast Join                                       = disabled,
Initial Packet Buffering                        = disabled,
    Max Flows                                   = 32,
    Max Packets Per Flow                        = 4,
    Buffer Timeout (seconds)                    = 10,
    Min Delay (milliseconds)                    = 0

-> show ip multicast vlan 200

Profile                                         = default,
Status                                          = disabled,
Flood Unknown                                   = disabled,
Version                                         = 2,
Robustness                                      = 2,
Querying                                        = disabled,
Query Interval (seconds)                        = 125,
Query Response Interval (tenths of seconds)     = 100,
Last Member Query Interval (tenths of seconds)  = 10,
Unsolicited Report Interval (seconds)           = 1,
Proxying                                        = disabled,
Spoofing                                        = disabled,
Zapping                                         = disabled,
Querier Forwarding                              = disabled,
Router Timeout (seconds)                        = 90,
Source Timeout (seconds)                        = 30,
Max-group                                       = 0,
Max-group action                                = none,
Helper-address                                  = 0.0.0.0,
Static Querier Address                          = 0.0.0.0,
Static Spoofer Address                          = 0.0.0.0,
Zero-based Query                                = disabled,
Forward Mode                                    = auto,
Update Delay Interval (milliseconds)            = 0,
SSM Mapping                                     = disabled,
Fast Join                                       = disabled,
Initial Packet Buffering                        = disabled,
    Max Flows                                   = 32,
    Max Packets Per Flow                        = 32,
    Buffer Timeout (seconds)                    = 10,
    Min Delay (milliseconds)                    = 0

-> show ip multicast service 20

Profile                                         = default,
Status                                          = disabled,
Flood Unknown                                   = disabled,
Version                                         = 2,
Robustness                                      = 2,
Querying                                        = disabled,
Query Interval (seconds)                        = 125,
Query Response Interval (tenths of seconds)     = 100,
Last Member Query Interval (tenths of seconds)  = 10,
Unsolicited Report Interval (seconds)           = 1,
Proxying                                        = disabled,
Spoofing                                        = disabled,
```

```
Zapping                                          = disabled,
Querier Forwarding                               = disabled,
Router Timeout (seconds)                         = 0,
Source Timeout (seconds)                         = 300,
Max-group                                        = 0,
Max-group action                                 = none,
Helper-address                                   = 0.0.0.0,
Static Querier Address                           = 0.0.0.0,
Static Spoofer Address                           = 0.0.0.0,
Zero-based Query                                 = disabled,
Forward Mode                                     = mac,
Update Delay Interval (milliseconds)             = 0,
SSM Mapping                                      = disabled,
Fast Join                                        = disabled,
Initial Packet Buffering                         = disabled,
    Max Flows                                    = 32,
    Max Packets Per Flow                         = 32,
    Buffer Timeout (seconds)                     = 10,
    Min Delay (milliseconds)                     = 0
```

output definitions

Profile	The name of a predefined IPMS configuration profile that is assigned to this instance. Configured through the **ip multicast profile** command.
Status	Whether IP Multicast Switching and Routing is **Enabled** or **Disabled** (the default status). Configured through the **ip multicast admin-state** command.
Flood Unknown	Whether the flooding of initial unknown multicast traffic is **Enabled** or **Disabled** (the default status). Configured through the **ip multicast flood-unknown** command.
Version	Displays the default IGMP version, which can be **1, 2** or **3**. Configured through the **ip multicast version** command.
Robustness	Displays the IGMP robustness value, ranging from **1** to **7.** (The default value is 2). Configured through the **ip multicast robustness** command.
Querying	Whether IGMP querying is **Enabled** or **Disabled** (the default status). Configured through the **ip multicast querying** command.
Query Interval (seconds)	Displays the time (in seconds) between IGMP queries. (The default value is 125 seconds). Configured through the **ip multicast query-interval** command.
Query Response Interval (tenths of seconds)	Displays the time (in tenths of seconds) taken to reply to an IGMP query message. (The default value is 100 tenths-of-seconds). Configured through the **ip multicast query-response-interval** command.
Last Member Query Interval (tenths of seconds)	Displays the time (in tenths of seconds) taken to reply to an IGMP query message sent in response to a leave group message. (The default value is 10 tenths-of-seconds.) Configured through the **ip multicast last-member-query-interval** command.
Unsolicited Report Interval (seconds)	Displays the time period (in seconds) to proxy any changed IGMP membership state. (The default value is 1 second). Configured through the **ip multicast unsolicited-report-interval** command.

output definitions

Proxying	Whether IGMP proxying on the system is **enabled** or **disabled** (the default status)**.** Configured through the **ip multicast proxying** command.
Spoofing	Whether IGMP spoofing on the system is **enabled** or **disabled** (the default status)**.** Configured through the **ip multicast spoofing** command.
Zapping	Whether IGMP zapping on the system is **enabled** or **disabled** (the default status)**.** Configured through the **ip multicast zapping** command.
Querier Forwarding	Whether IGMP querier forwarding on the system is **enabled** or **disabled** (the default status)**.** Configured through the **ip multicast querier-forwarding** command.
Router Timeout (seconds)	Displays the IGMP router timeout in seconds. (The default value is 90 seconds.) Configured through the **ip multicast router-timeout** command.
Source Timeout (seconds)	Displays the IGMP source timeout in seconds. (The default value is 30 seconds.) Configured through the **ip multicast source-timeout** command.
Max-group	Displays the global maximum group limit that can be learned per VLAN instance. (The default value is 0, which means no limit is imposed). Configured through the **ip multicast max-group** command.
Max-group action	Displays the action taken when the maximum group limit has been exceeded (**none**, **drop** or **replace**). Configured through the **ip multicast max-group** command.
Helper-address	Displays the destination IP address of a relay host, where IGMP host reports and Leave messages are to be sent. (By default, no Helper-address is configured.) Configured through the **ip multicast helper-address** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Static Querier Address	The Static Source IP Address to be used when querying. (The default value of 0.0.0.0 indicates that this is not configured.) *This function is currently not supported.*
Static Spoofing Address	The Static Source IP Address to be used when spoofing. (The default value of 0.0.0.0 indicates that this is not configured.) Configured through the **ip multicast spoofing static-source-ip** command.
Zero-based Query	Whether Zero-based Querying is **disabled** or **enabled** (the default status). Configured through the **ip multicast zero-based-query** command.
Forward Mode	Displays the current IPv4 Forwarding mode (**asm**, **ssm**, **mac**, or **auto**). Configured through the **ip multicast forward-mode** command.
Update Delay Interval (milliseconds)	Displays the amount of time (in milliseconds) between propagating IPMS state changes. (The default value is 0 milliseconds). Configured through the **ip multicast update-delay-interval** command.

output definitions

SSM Mapping	Whether Source Specific Multicast (SSM) mapping is **enabled** or **disabled** (the default). When enabled, Any Source Multicast (ASM) group memberships are translated into SSM group memberships. Configured through the **ip multicast ssm-map** command. *This function is currently not supported.*
Fast Join	Whether the IP Multicast Switching fast join functionality is **enabled** or **disabled** (the default). When enabled, forwarding entries are automatically created in hardware as soon as IGMP memberships are learned instead of waiting for the multicast traffic to reach the switch. Configured through the **ip multicast fast-join** command.
Initial Packet Buffering	The current state of Initial Packet Buffering, which can be **enabled** or **disabled** (the default status). Configured through the **ip multicast initial-packet-buffer admin-state** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Max Flows	The maximum number of IPv4 multicast flows buffered for initial packet. Configured through the **ip multicast initial-packet-buffer max-flow** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Max Packets Per Flow	The maximum number of initial packets buffered per IPv4 multicast flow. Configured through the **ip multicast initial-packet-buffer max-packet** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Buffer Timeout (seconds)	The timeout value for the initial buffered IPv4 multicast packets. Configured through the **ip multicast initial-packet-buffer timeout** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Min Delay (milliseconds)	The minimum delay to program the multicast replication index for IPv4 multicast flows buffered for initial packet. Configured through the **ip multicast initial-packet-buffer min-delay** command. *This function is supported only in the VLAN domain; service domain is not supported.*

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; display fields added.
Release 8.4.1; **service** parameter added.

Related Commands

ip multicast admin-state	Enables or disables IP Multicast Switching and Routing on the specified VLAN, or on the system if no VLAN is specified.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigStatus
   alaIpmsConfigQuerying
   alaIpmsConfigProxying
   alaIpmsConfigSpoofing
   alaIpmsConfigZapping
   alaIpmsConfigQuerierForwarding
   alaIpmsConfigVersion
   alaIpmsConfigRobustness
   alaIpmsConfigQueryInterval
   alaIpmsConfigQueryResponseInterval
   alaIpmsConfigLastMemberQueryInterval
   alaIpmsConfigUnsolicitedReportInterval
   alaIpmsConfigRourceTimeout
   alaIpmsConfigSourceTimeout
   alaIpmsConfigMaxGroupLimit
   alaIpmsConfigMaxGroupExceedAction
   alaIpmsConfigZeroBasedQuery
   alaIpmsConfigStaticSsmMapping
   alaIpmsConfigFloodUnknown
   alaIpmsConfigUpdateDelayInterval
   alaIpmsConfigForwardMode
   alaIpmsConfigQueryingStaticSourceAddress
   alaIpmsConfigSpoofingStaticSourceAddress
   alaIpmsConfigInitialPacketBuffer
   alaIpmsConfigInitialPacketBufferMaxPacket
   alaIpmsConfigInitialPacketBufferMaxFlow
   alaIpmsConfigInitialPacketBufferTimeout
   alaIpmsConfigInitialPacketBufferMinDelay
   alaIpmsConfigHelperAddress
   alaIpmsConfigFastJoin
```

show ip multicast port

Displays the maximum group configuration applicable for the specified port or the specified Service Access Point (SAP) port. The current number of groups learned on a port, port/VLAN, SAP port, or SAP port/Shortest Path Bridging (SPB) service instance is also displayed.

show ip multicast {port [*chassis/slot/port***] | sap port** [*sap_id*]}

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
sap_id	The SAP ID (chassis/slot/port:encapsulation). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify a port number to display the configuration information for a specific switch port.
- Specify a SAP ID to display the configuration information for a specific SAP port.
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ip multicast static-querier service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID).
- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

Examples

```
-> show ip multicast port

Legends: Interface Max-group          = Max-group limit on the interface
         Interface Action             = Max-group action on the interface
         Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
         Interface-Instance Action    = Active Max-group action on the Lan Interface instance

Total 2 Lan Interface Instances

Interface      Vlan/Service Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
--------------+------------+-------+---------+---------+------------------+------------------
1/1/13         vlan 1036    0       0         none      0                  none
1/1/52         vlan 1       0       0         none      0                  none
```

```
-> show ip multicast port 1/1/52

Legends: Interface Max-group          = Max-group limit on the interface
         Interface Action             = Max-group action on the interface
         Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
         Interface-Instance Action    = Active Max-group action on the Lan Interface instance

Total 2 Lan Interface Instances

Interface      Vlan/Service Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
--------------+------------+-------+---------+---------+------------------+------------------
1/1/52         vlan 1       0       0         none      0                  none

-> show ip multicast sap port

Legends: Interface Max-group          = Max-group limit on the interface
         Interface Action             = Max-group action on the interface
         Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
         Interface-Instance Action    = Active Max-group action on the Lan Interface instance

Total 2 Lan Interface Instances

Interface      Vlan/Service Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
--------------+------------+-------+---------+---------+------------------+------------------
sap:1/1/5:100  service 20   0       0         none      0                  none
sap:1/1/23:200 service 30   0       0         none      0                  none

-> show ip multicast sap port 1/1/23:200

Legends: Interface Max-group          = Max-group limit on the interface
         Interface Action             = Max-group action on the interface
         Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
         Interface-Instance Action    = Active Max-group action on the Lan Interface instance

Total 2 Lan Interface Instances

Interface      Vlan/Service Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
--------------+------------+-------+---------+---------+------------------+------------------
sap:1/1/23:200 service 30   0       0         none      0                  none
```

output definitions

Interface	The VLAN port or the SAP (chassis/slot/port:encapsulation) that serves as the virtual port for the SPB service.
Vlan/Service	The VLAN or SPB service ID associated with the IP multicast interface.
Current Groups	The current groups associated with the IP multicast interface.
Interface Max-group	The maximum group count allowed on the port or SAP port. This limit is applicable on the given port for all VLAN or service instances of the port.
Interface Action	The action to be taken when the group membership limit is exceeded (**none**, **drop**, or **replace**).

output definitions

Interface-Instance Max-group	The maximum group limit learned per port for the given VLAN or per SAP port for the given SPB service. This limit is applied to each port that is a member of the given VLAN or each SAP port that is a member of the given service.
Interface-Instance Action	The action to be taken when the group membership limit is exceeded (**none**, **drop**, or **replace**).

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **sap port** parameter added.

Related Commands

ip multicast port max-group	Configures the maximum group limit learned per port.
ip multicast port max-group	Configures the maximum group limit learned per port for the specified VLAN, SPB service, or on the system if no VLAN or SPB service is specified.

MIB Objects

```
alaIpmsIntfStatsConfigType
   alaIpmsIntfStatsAddressType
   alaIpmsIntfStatsValue
   alaIpmsIntfStatsCurrentGroupCount
   alaIpmsIntfStatsMaxGroupLimit
   alaIpmsIntfStatsMaxGroupExceedAction
```

show ip multicast forward

Displays the IP Multicast Switching and Routing forwarding table entries for the specified IP multicast group address or all the entries if no IP multicast group address is specified.

show ip multicast forward [*ip_address***] [vlan [***vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

ip_address	IP multicast group address.
vlan [*vlan_id***[-***vlan_id2***]**	Display forwarding table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display forwarding table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display forwarding table entries for all of the VRF instances.

Defaults

By default, forwarding entries for all of the IP multicast groups are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ip_address* parameter to display forwarding table entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the forwarding table entries that exist in all of the VRF instances on the switch.
- Forwarding entries are derived by applying the state from the source table to the state in the group, neighbor, and querier tables.
- On an OmniSwitch 9900, this command is available only when IP Multicast Switching *and* Routing is enabled for the switch. To view the multicast forwarding database on an OS6465 or OS6560 see the **show ip multicast bridge** and **show ip multicast bridge-forward** commands.
- Use the **ip multicast display-interface-names** command to enable displaying the associated IP interface name in the “Ingress Vlan/Service” and “Egress Vlan/Service” fields instead of the VLAN ID or service ID.

Examples

```
-> show ip multicast forward

Total 3 Forwards
                                                 Ingress      Egress
Group Address   Host Address   Tunnel Address Vlan/Service Vlan/Service Interface
---------------+--------------+--------------+------------+------------+----------
225.0.1.0       21.20.20.2     0.0.0.0        vlan 20      vlan 20      1/1/2
225.0.1.0       21.20.20.2     0.0.0.0        service 10   service 10   sdp:32776
225.0.1.1       21.20.20.2     0.0.0.0        vlan 20      vlan 20      1/1/2
225.0.1.1       21.20.20.2     0.0.0.0        service 10   service 10   sdp:32776
225.0.1.2       21.20.20.2     0.0.0.0        vlan 20      vlan 21      1/1/2
225.0.1.2       21.20.20.2     0.0.0.0        service 10   service 10   sap:1/5:10

-> show ip multicast forward service

Total 3 Forwards
                                                 Ingress      Egress
Group Address   Host Address   Tunnel Address Vlan/Service Vlan/Service Interface
---------------+--------------+--------------+------------+------------+----------
225.0.1.0       21.20.20.2     0.0.0.0        service 10   service 10   sdp:32776
225.0.1.1       21.20.20.2     0.0.0.0        service 10   service 10   sdp:32776
225.0.1.2       21.20.20.2     0.0.0.0        service 10   service 10   sap:1/5:10

-> show ip multicast forward vlan

Total 3 Forwards
                                                 Ingress      Egress
Group Address   Host Address   Tunnel Address Vlan/Service Vlan/Service Interface
---------------+--------------+--------------+------------+------------+----------
225.0.1.0       21.20.20.2     0.0.0.0        vlan 20      vlan 20      1/1/2
225.0.1.1       21.20.20.2     0.0.0.0        vlan 20      vlan 20      1/1/2
225.0.1.2       21.20.20.2     0.0.0.0        vlan 20      vlan 21      1/1/2
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast forward vlan

Total 3 Forwards
                                                 Ingress      Egress
Group Address   Host Address   Tunnel Address Vlan/Service Vlan/Service Interface
---------------+--------------+--------------+------------+------------+----------
225.0.1.0       21.20.20.2     0.0.0.0        VlanToLab    VlanToLab    1/1/2
225.0.1.1       21.20.20.2     0.0.0.0        VlanToLab    VlanToLab    1/1/2
225.0.1.2       21.20.20.2     0.0.0.0        VlanToLab    VlanToCore   1/1/2
```

output definitions

Group Address	IP group address of the IP multicast forward.
Host Address	IP host address of the IP multicast forward.
Tunnel Address	IP source tunnel address of the IP multicast forward.
Ingress Vlan/Service	The ingress VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast forward. If the global display interface names option is enabled, then the ingress interface name associated with the IP multicast forward is displayed.

output definitions (continued)

Egress Vlan/Service	The egress VLAN or SPB service ID associated with the IP multicast forward. If the global display interface names option is enabled, then the egress interface name associated with the IP multicast forward is displayed. The egress interface (port) will also be included in the forward entry with both output formats.
Interface	The VLAN port or SPB virtual port of the IP multicast forward.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

ip multicast static-group	Creates a static IGMP group entry on a specified port on a specified VLAN.

MIB Objects

```
alaIpmsForwardTable
   alaIpmsForwardConfigType
   alaIpmsForwardAddressType
   alaIpmsForwardValue
   alaIpmsForwardGroupAddress
   alaIpmsForwardHostAddress
   alaIpmsForwardDestAddress
   alaIpmsForwardOrigAddress
   alaIpmsForwardType
   alaIpmsForwardNextConfigType
   alaIpmsForwardNextValue
   alaIpmsForwardNextIfIndex
   alaIpmsForwardNextType
```

show ip multicast neighbor

Displays the IGMP neighbor table entries of IP Multicast Switching and Routing.

show ip multicast neighbor [vlan [*vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

vlan [*vlan_id***[-***vlan_id2***]**	Display IGMP neighbor table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display IGMP neighbor table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display IGMP neighbor table entries for all of the VRF instances.

Defaults

By default, only the neighbor table entries specific to the current VRF instance are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **all-vrf** parameter option to display the neighbor table entries that exist in all of the VRF instances on the switch.
- Interfaces with neighbors receive all IPv4 multicast, including all IGMP traffic.
- Use the **ip multicast display-interface-names** command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ip multicast neighbor

Total 12 Neighbors

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
170.0.0.2        vlan 2000   0/10       no      528    85
170.0.1.3        vlan 2001   0/1        no      502    66
170.0.59.45      vlan 2059   0/11       no      554    80
170.0.61.46      vlan 2061   0/12       no      553    79
170.0.63.47      vlan 2063   0/13       no      553    66
170.0.65.48      vlan 2065   0/14       no      553    64
170.0.67.51      vlan 2067   1/5/31     no      475    86
170.0.69.52      vlan 2069   1/5/43     no      553    83
170.0.71.53      vlan 2071   1/6/31     no      552    61
170.0.73.54      vlan 2073   1/6/43     no      552    67
225.0.1.0        service 20  SAP:1/5:10 no      5520   172
```

```
225.0.1.0        service 20  SAP:1/5:20 no      5520   172

-> show ip multicast neighbor service

Total 2 Neighbors

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
225.0.1.0        service 20  SAP:1/5:10 no      5520   172
225.0.1.0        service 20  SAP:1/5:20 no      5520   172

-> show ip multicast neighbor vlan

Total 10 Neighbors

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
170.0.0.2        vlan 2000   0/10       no      528    85
170.0.1.3        vlan 2001   0/1        no      502    66
170.0.59.45      vlan 2059   0/11       no      554    80
170.0.61.46      vlan 2061   0/12       no      553    79
170.0.63.47      vlan 2063   0/13       no      553    66
170.0.65.48      vlan 2065   0/14       no      553    64
170.0.67.51      vlan 2067   1/5/31     no      475    86
170.0.69.52      vlan 2069   1/5/43     no      553    83
170.0.71.53      vlan 2071   1/6/31     no      552    61
170.0.73.54      vlan 2073   1/6/43     no      552    67

-> show ip multicast neighbor vlan 2063

Total 1 Neighbors

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
170.0.63.47      vlan 2063   0/13       no      553    66
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast neighbor vlan 2063

Total 1 Neighbors

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
170.0.63.47      VlanToLab   0/13       no      553    66
```

output definitions

Host Address	The IP address of the IP multicast neighbor.
Vlan/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast neighbor. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast neighbor is displayed.
Interface	The VLAN port or the SPB virtual port of the IP multicast neighbor.

output definitions

Static	Whether it is a static IP multicast neighbor or not.
Count	Displays the count of IP multicast neighbor.
Life	The life time of the IP multicast neighbor.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

ip multicast static-neighbor	Creates a static IGMP neighbor entry on a specified port on a specified VLAN.

MIB Objects

```
alaIpmsNeighborTable
   alaIpmsNeighborConfigType
   alaIpmsNeighborAddressType
   alaIpmsNeighborValue
   alaIpmsNeighborIfIndex
   alaIpmsNeighborHostAddress
   alaIpmsNeighborCount
   alaIpmsNeighborTimeout
   alaIpmsNeighborUpTime
alaIpmsStaticNeighborTable
   alaIpmsStaticNeighborConfigType
   alaIpmsStaticNeighborAddressType
   alaIpmsStaticNeighborValue
   alaIpmsStaticNeighborIfIndex
   alaIpmsStaticNeighborRowStatus
```

show ip multicast querier

Displays the IGMP querier table entries of IP Multicast Switching and Routing.

show ip multicast querier [vlan [*vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

vlan [*vlan_id***[-***vlan_id2***]**	Display IGMP querier table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display IGMP querier table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display IGMP querier table entries for all of the VRF instances.

Defaults

By default, only IGMP querier entries specific to the current VRF instance are displayed

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **all-vrf** parameter option to display the IGMP querier table entries that exist in all of the VRF instances on the switch.
- Interfaces with queriers receive all IGMP traffic, and if querier forwarding is enabled, these interfaces will also receive all IPv4 multicast traffic.
- Use the **ip multicast display-interface-names** command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ip multicast querier

Total 10 Queriers

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
172.1.254.96     vlan 1001   0/1        no      3      213
172.2.254.96     vlan 1002   0/1        no      4      213
172.3.254.96     vlan 1003   0/1        no      4      214
172.4.254.96     vlan 1004   0/1        no      4      213
172.5.254.96     vlan 1005   0/1        no      4      213
172.6.254.96     vlan 1006   0/1        no      4      213
172.7.254.96     vlan 1007   0/1        no      4      213
172.8.254.96     vlan 1008   0/1        no      4      213
225.0.1.0        service 10  SAP:1/5:10 no      5520   172
225.0.1.0        service 10  SAP:1/5:20 no      5520   172
```

```
-> show ip multicast querier service

Total 2 Queriers

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
225.0.1.0       service 10   SAP:1/5:10 no      5520   172
225.0.1.0       service 10   SAP:1/5:20 no      5520   172

-> show ip multicast querier vlan

Total 8 Queriers

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
172.1.254.96     vlan 1001   0/1        no      3      213
172.2.254.96     vlan 1002   0/1        no      4      213
172.3.254.96     vlan 1003   0/1        no      4      214
172.4.254.96     vlan 1004   0/1        no      4      213
172.5.254.96     vlan 1005   0/1        no      4      213
172.6.254.96     vlan 1006   0/1        no      4      213
172.7.254.96     vlan 1007   0/1        no      4      213
172.8.254.96     vlan 1008   0/1        no      4      213
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast querier vlan

Total 8 Queriers

Host Address    Vlan/Service Interface  Static  Count  Life
---------------+------------+----------+-------+------+-----
172.1.254.96     VlanToLab    0/1        no      3      213
172.2.254.96     VlanToLab    0/1        no      4      213
172.3.254.96     VlanToLab    0/1        no      4      214
172.4.254.96     VlanToLab    0/1        no      4      213
172.5.254.96     VlanToLab    0/1        no      4      213
172.6.254.96     VlanToLab    0/1        no      4      213
172.7.254.96     VlanToLab    0/1        no      4      213
172.8.254.96     VlanToLab    0/1        no      4      213
```

output definitions

Host Address	The IP address of the IP multicast querier.
Vlan/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast querier. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast querier is displayed.
Interface	The VLAN port or the SPB virtual port of the IP multicast querier.
Static	Whether it is a static multicast neighbor or not.
Count	Displays the count of the IP multicast querier.
Life	The life time of the IP multicast querier.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

ip multicast static-querier	Creates a static IGMP querier entry on a specified port on a specified VLAN.

MIB Objects

```
alaIpmsQuerierTable
   alaIpmsQuerierConfigType
   alaIpmsQuerierAddressType
   alaIpmsQuerierValue
   alaIpmsQuerierIfIndex
   alaIpmsQuerierHostAddress
   alaIpmsQuerierCount
   alaIpmsQuerierTimeout
   alaIpmsQuerierUpTime
alaIpmsStaticQuerierTable
   alaIpmsStaticQuerierConfigType
   alaIpmsStaticQuerierAddressType
   alaIpmsStaticQuerierValue
   alaIpmsStaticQuerierIfIndex
   alaIpmsStaticQuerierRowStatus
```

show ip multicast group

Displays the IGMP group membership table entries of IP Multicast Switching and Routing for the specified IP multicast group address or all entries if no IP multicast group address is specified.

show ip multicast group [*ip_address***] [vlan [***vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

ip_address	IP multicast group address.
vlan [*vlan_id***[-***vlan_id2***]**	Display group membership entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display group membership entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display group membership entries for all of the VRF instances.

Defaults

By default, all IP multicast groups are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ip_address* parameter to display entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the IGMP group membership table entries that exist in all of the VRF instances on the switch.
- Use the **ip multicast display-interface-names** command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ip multicast group

Total 8 Groups

Group Address   Source Address  Vlan/Service   Interface        Mode     Static  Count  Life
----------------+---------------+--------------+----------------+--------+-------+------+-----
225.0.1.0       0.0.0.0         vlan 21        1/1/19           exclude  no      5520   172
225.0.1.0       0.0.0.0         service 20     SAP:1/5:10       exclude  no      5520   172
225.0.1.0       0.0.0.0         service 20     SAP:1/5:20       exclude  no      5520   172
225.0.1.0       0.0.0.0         service 20     sdp:32776        exclude  no      5520   172
225.0.1.1       0.0.0.0         vlan 21        1/1/19           exclude  no      5520   172
225.0.1.2       0.0.0.0         vlan 21        1/1/19           exclude  no      5520   172
225.0.1.3       0.0.0.0         vlan 100       1/1/1            exclude  yes     0      0
225.0.1.4       0.0.0.0         vlan 101       1/1/1            exclude  yes     0      0
```

```
-> show ip multicast group 225.0.1.0

Total 1 Groups

Group Address   Source Address  Vlan/Service   Interface        Mode     Static  Count  Life
---------------+---------------+--------------+----------------+--------+-------+------+-----
225.0.1.0       0.0.0.0         vlan 21        1/1/19           exclude  no      5520   172
225.0.1.0       0.0.0.0         service 20     SAP:1/5:10       exclude  no      5520   172
225.0.1.0       0.0.0.0         service 20     SAP:1/5:20       exclude  no      5520   172
225.0.1.0       0.0.0.0         service 20     sdp:32776        exclude  no      5520   172

-> show ip multicast group service

Total 3 Groups

Group Address   Source Address  Vlan/Service   Interface        Mode     Static  Count  Life
---------------+---------------+--------------+----------------+--------+-------+------+-----
225.0.1.0       0.0.0.0         service 20     SAP:1/5:10       exclude  no      5520   172
225.0.1.0       0.0.0.0         service 20     SAP:1/5:20       exclude  no      5520   172
225.0.1.0       0.0.0.0         service 20     sdp:32776        exclude  no      5520   172

-> show ip multicast group vlan

Total 5 Groups

Group Address   Source Address  Vlan/Service   Interface        Mode     Static  Count  Life
---------------+---------------+--------------+----------------+--------+-------+------+-----
225.0.1.0       0.0.0.0         vlan 21        1/1/19           exclude  no      5520   172
225.0.1.1       0.0.0.0         vlan 21        1/1/19           exclude  no      5520   172
225.0.1.2       0.0.0.0         vlan 21        1/1/19           exclude  no      5520   172
225.0.1.3       0.0.0.0         vlan 100       1/1/1            exclude  yes     0      0
225.0.1.4       0.0.0.0         vlan 101       1/1/1            exclude  yes     0      0
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast group vlan

Total 5 Groups

Group Address   Source Address  Vlan/Service   Interface        Mode     Static  Count  Life
---------------+---------------+--------------+----------------+--------+-------+------+-----
225.0.1.0       0.0.0.0         VlanToLab      1/1/19           exclude  no      5520   172
225.0.1.1       0.0.0.0         VlanToLab      1/1/19           exclude  no      5520   172
225.0.1.2       0.0.0.0         VlanToLab      1/1/19           exclude  no      5520   172
225.0.1.3       0.0.0.0         VlanToCore     1/1/1            exclude  yes     0      0
225.0.1.4       0.0.0.0         VlanToDist     1/1/1            exclude  yes     0      0
```

output definitions

Group Address	IP address of the IP multicast group.
Source Address	IP address of the IP multicast source.
Vlan/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IPv4 multicast group. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast group is displayed.
Interface	The VLAN port or the SPB virtual port on which the group membership was learned.
Mode	IGMP source filter mode.

output definitions

Static	Whether it is a static multicast group or not.
Count	Number of IGMP membership requests made.
Life	Life time of the IGMP group membership.

Release History

Release 7.1.1; command was introduced
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands.

ip multicast static-group	Creates a static IGMP group entry on a specified port for the specified VLAN or on the specified SPB virtual port for the specified SPB service.

MIB Objects

```
alaIpmsMemberTable
   alaIpmsMemberConfigType
   alaIpmsMemberAddressType
   alaIpmsMemberValue
   alaIpmsMemberIfIndex
   alaIpmsMemberGroupAddress
   alaIpmsMemberSourceAddress
   alaIpmsMemberMode
   alaIpmsMemberCount
   alaIpmsMemberTimeout
 alaIpmsStaticMemberTable
   alaIpmsStaticMemberConfigType
   alaIpmsStaticMemberConfigAddressType
   alaIpmsStaticMemberValue
   alaIpmsStaticMemberIfIndex
   alaIpmsStaticMemberGroupAddress
   alaIpmsStaticMemberRowStatus
```

show ip multicast source

Displays the IP Multicast Switching and Routing source table entries matching the specified IP multicast group address or all entries if no IP multicast group address is specified.

show ip multicast source [*ip_address***] [vlan [***vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***] [all-vrf]**

Syntax Definitions

ip_address	IP multicast group address.
vlan [*vlan_id***[-***vlan_id2***]**	Displays source table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Displays source table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display source table entries for all of the VRF instances.

Defaults

By default, all source table entries are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ip_address* parameter to display source entries for a specific multicast group.
- In the service domain, only the first flow that is used to learn the source is displayed. Use the **extended** parameter to display other possible multicast IP addresses matching the same multicast MAC address. In this case, an asterisk (*) in the “Host Address” field represents the other multicast IP addresses.
- Use the **all-vrf** parameter option to display the source table entries that exist in all of the VRF instances on the switch.
- On an OmniSwitch 9900, this command is available only when IP Multicast Switching *and* Routing is enabled for the switch. To view the multicast forwarding database on an OS6465 or OS6560 see the **show ip multicast bridge** and **show ip multicast bridge-forward** commands.
- Use the **ip multicast display-interface-names** command to enable displaying the associated IP interface name in the “Ingress Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ip multicast source

Total 10 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
225.0.1.0       21.20.20.2      0.0.0.0         vlan 21
225.0.1.0       21.20.20.2      0.0.0.0         service 20
225.0.1.1       21.20.20.2      0.0.0.0         vlan 21
225.0.1.1       21.20.20.2      0.0.0.0         service 20
225.0.1.2       21.20.20.2      0.0.0.0         vlan 21
225.0.1.2       21.20.20.2      0.0.0.0         service 20
225.0.1.3       21.20.20.2      0.0.0.0         vlan 21
225.0.1.3       21.20.20.2      0.0.0.0         service 20
225.0.1.4       21.20.20.2      0.0.0.0         vlan 21
225.0.1.4       21.20.20.2      0.0.0.0         service 20

-> show ip multicast source 225.0.1.2

Total 2 Sources
                                    Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
225.0.1.2       21.20.20.2      0.0.0.0         vlan 21
225.0.1.2       21.20.20.2      0.0.0.0         service 20

-> show ip multicast source service

Total 5 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
225.0.1.0       21.20.20.2      0.0.0.0          20
225.0.1.1       21.20.20.2      0.0.0.0          20
225.0.1.2       21.20.20.2      0.0.0.0          20
225.0.1.3       21.20.20.2      0.0.0.0          20
225.0.1.4       21.20.20.2      0.0.0.0          20

-> show ip multicast source vlan

Total 5 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
225.0.1.0       21.20.20.2      0.0.0.0         vlan 21
225.0.1.1       21.20.20.2      0.0.0.0         vlan 21
225.0.1.2       21.20.20.2      0.0.0.0         vlan 21
225.0.1.3       21.20.20.2      0.0.0.0         vlan 21
225.0.1.4       21.20.20.2      0.0.0.0         vlan 21
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast source vlan

Total 5 Sources

                                      Source        Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
225.0.1.0       21.20.20.2      0.0.0.0         VlanToLab
225.0.1.1       21.20.20.2      0.0.0.0         VlanToLab
225.0.1.2       21.20.20.2      0.0.0.0         VlanToLab
225.0.1.3       21.20.20.2      0.0.0.0         VlanToLab
225.0.1.4       21.20.20.2      0.0.0.0         VlanToLab
```

output definitions

Group Address	IP group address of the IP multicast source.
Host Address	IP host address of the IP multicast source.
Source Tunnel Address	IP destination tunnel address of the IP multicast source.
Ingress Vlan/Service	The ingress VLAN or Shortest Path Bridging (SPB) service ID number associated with the IP multicast source. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast source is displayed.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

show ip multicast tunnel	Display the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

MIB Objects

```
alaIpmsSourceTable
   alaIpmsSourceConfigType
   alaIpmsSourceAddressType
   alaIpmsSourceValue
   alaIpmsSourceGroupAddress
   alaIpmsSourceHostAddress
   alaIpmsSourceDestAddress
   alaIpmsSourceOrigAddress
   alaIpmsSourceType
   alaIpmsSourceUpTime
```

show ip multicast tunnel

Displays the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

show ip multicast tunnel [*ip_address***] [vlan [***vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

ip_address	IP multicast group address.
vlan [*vlan_id***[-***vlan_id2***]**	Displays tunneling table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Displays tunneling table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display the tunneling table entries for all of the VRF instances.

Defaults

By default, all tunnel entries are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ip_address* parameter to display the tunnel entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the IP multicast tunnel entries that exist in all of the VRF instances on the switch.
- Use the **ip multicast display-interface-names** command to enable displaying the associated IP interface name in the “Ingress Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ip multicast tunnel

Total 3 Tunnels
                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
--------------+---------------+---------------+-------------
225.0.1.0       21.20.20.2      10.10.10.51     vlan 20
225.0.1.1       21.20.20.2      10.10.10.51     vlan 20
225.0.1.2       21.20.20.2      10.10.10.51     vlan 20
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast tunnel

Total 3 Tunnels
                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
--------------+---------------+---------------+--------------
225.0.1.0       21.20.20.2      10.10.10.51     VlanToLab
225.0.1.1       21.20.20.2      10.10.10.51     VlanToLab
225.0.1.2       21.20.20.2      10.10.10.51     VlanToLab
```

output definitions

Group Address	IP group address of the IP multicast tunnel.
Host Address	IP host address of the IP multicast tunnel.
Destination Tunnel Address	IP source tunnel address of the IP multicast tunnel.
Ingress Vlan/Service	VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast tunnel. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast tunnel is displayed.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1.R02: **vlan** and **service** parameters added.

Related Commands

show ip multicast source	Displays the IP Multicast Switching and Routing source table entries matching the specified IP multicast group address or all entries if no IP multicast group address is specified

MIB Objects

```
alaIpmsTunnelTable
   alaIpmsTunnelConfigType
   alaIpmsTunnelAddressType
   alaIpmsTunnelValue
   alaIpmsTunnelGroupAddress
   alaIpmsTunnelHostAddress
   alaIpmsTunnelDestAddress
   alaIpmsTunnelOrigAddress
   alaIpmsTunnelType
   alaIpmsTunnelNextDestAddress
   alaIpmsTunnelNextType
```

show ip multicast host-list

Displays the IP multicast host address list configuration for the switch.

show ip multicast host-list [*host_list_name***]**

Syntax Definitions

host_list_name	The name of an existing IP multicast host list.

Defaults

By default, all host lists configured on the switch are displayed.

Platforms Supported

Not supported in this release.

Usage Guidelines

Use the *host_list_name* parameter to display information for a specific host list.

Examples

```
-> show ip multicast host-list

Total 2 Lists

Host List Name                   Addresses
---------------------------------+---------------
group-map1                       10.2.2.1
                                 10.2.2.3
                                 10.2.2.4
                                 10.2.2.5
ssm-map1                         20.2.2.1
                                 20.2.2.2
                                 20.2.2.3

-> show ip multicast host-list ssm-map1

Host List Name                   Addresses
---------------------------------+---------------
ssm-map1                         20.2.2.1
                                 20.2.2.2
                                 20.2.2.3
```

Release History

Release 8.3.1.R02; command introduced.

Related Commands

ip multicast host-list	Configures a list of host IP addresses that is used for IP multicast group maps and SSM maps.

MIB Objects

```
alaIpmsHostListTable
   alaIpmsHostListName
   alaIpmsHostListAddressType
   alaIpmsHostListAddress
```

show ip multicast ssm-map

Displays the Source Specific Multicast (SSM) mapping configuration for the switch.

show ip multicast ssm-map [vlan *vlan_id***]**

Syntax Definitions

vlan_id	VLAN for which to display the configuration.

Defaults

By default, all SSM mappings configured on the switch are displayed.

Platforms Supported

Not supported in this release.

Usage Guidelines

Specify a VLAN ID to display the configuration information for a specific VLAN.

Examples

```
-> show ip multicast ssm-map
Type    Id    Group Address/Prefix  Source List Name
-------+-----+---------------------+--------------------------------
global  0     225.20.1.1/32         h-list1
vlan    200   229.30.1.1/32         h-list2

-> show ip multicast ssm-map vlan 200
Type    Id    Group Address/Prefix  Source List Name
-------+-----+---------------------+--------------------------------
vlan    200   229.30.1.1/32         h-list2
```

Release History

Release 8.3.1.R02; command introduced.

Related Commands

ip multicast ssm-map	Configures a list of host IP addresses.

MIB Objects

```
alaIpmsSsmMapTable
   alaIpmsSsmMapConfigType
   alaIpmsSsmMapConfigAddressType
   alaIpmsSsmMapConfigValue
   alaIpmsSsmMapGroupAddress
   alaIpmsSsmMapGroupPrefixLength
   alaIpmsSsmMapSourceListName
```

show ip multicast bridge

Displays the IP multicast bridge table entries that match the specified VLAN, Shortest Path Bridging (SPB) service, IP multicast group address, MAC address, or all entries if no additional parameters are specified.

show ip multicast bridge [vlan [*vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***] |** *ip_address* **|** *mac_address***] [all-vrf]**

Syntax Definitions

vlan [*vlan_id***[-***vlan_id2***]**	Displays bridge table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Displays bridge table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465 and OmniSwitch 6560.*
ip_address	IP multicast group address.
mac_address	Group MAC address.
all-vrf	Display bridge table entries for all of the VRF instances.

Defaults

By default, all bridge table entries are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6465, 6560, 9900

Usage Guidelines

- Use one of the optional parameters (*vlan_id*, *service_id*, *ip_address*, *mac_address*) to display bridge table entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the source table entries that exist in all of the VRF instances on the switch.
- Based on the forwarding mode set for the switch (ASM, SSM, or MAC):
  - The “Group Address” field will display either a multicast group address (ASM or SSM) or the MAC address for the multicast group (MAC).
  - The “Host Address” field will display zero (MAC) or the IP host address for the bridge entry (ASM or SSM).

Examples

```
-> show ip multicast bridge

Total 2 Bridge Entries

Vlan/Service   Type      Group Address     Host Address Action      UpTime
--------------+---------+-----------------+------------+-----------+---------------
vlan 1         asm       224.1.2.3                      forwarding  00d:00h:00m
vlan 10        mac       01-00-5e-09-08-07              forwarding  00d:00h:00m

-> show ip multicast bridge vlan 10

Total 1 Bridge Entries

Vlan/Service   Type      Group Address     Host Address Action      UpTime
--------------+---------+-----------------+------------+-----------+---------------
vlan 10        mac       01-00-5e-09-08-07              forwarding  00d:00h:00m
```

output definitions

Vlan/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast bridge entry.
Type	The bridge entry type (**asm**, **ssm**, **mac**). Configured through the **ip multicast forward-mode** command.
Group Address	If the bridge entry type is ASM or SSM, this field displays the destination IP group address; if the bridge entry type is MAC, this field displays the destination MAC address.
Host Address	The source IP host address (only applies to SSM bridge entries, otherwise this field is blank).
Action	The current action taken for the bridge entry (**forwarding** or **filtering**).
UpTime	The amount of time that has elapsed since the bridge entry was created.

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02: **service** parameter added.

Related Commands

show ip multicast bridge-forward	Displays the forwarding state of the IP multicast bridge table entries.

MIB Objects

```
alaIpmsBridgeTable
   alaIpmsBridgeConfigType
   alaIpmsBridgeAddressType
   alaIpmsBridgeValue
   alaIpmsBridgeType
   alaIpmsBridgeGroupAddress
   alaIpmsBridgeHostAddress
   alaIpmsBridgeUpTime
   alaIpmsBridgeAction
```

show ip multicast bridge-forward

Displays the forwarding state of the IP multicast bridge table entries that match the specified VLAN, Shortest Path Bridging (SPB) service, IP multicast group address, MAC address, or all entries if no additional parameters are specified.

show ip multicast bridge-forward [vlan [*vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***] |** *ip_address* **|** *mac_address***] [all-vrf]**

Syntax Definitions

vlan [*vlan_id***[-***vlan_id2***]**	Displays bridge table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Displays bridge table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465 and OmniSwitch 6560.*
ip_address	IP multicast group address.
mac_address	Group MAC address.
all-vrf	Display bridge table entries for all of the VRF instances.

Defaults

By default, all bridge table entries are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6465, 6560, 9900

Usage Guidelines

- Use one of the optional parameters (*vlan_id*, *service_id*, *ip_address*, *mac_address*) to display forwarding information for a specific multicast group.
- Use the **all-vrf** parameter option to display the source table entries that exist in all of the VRF instances on the switch.
- Based on the forwarding mode set for the switch (ASM, SSM, or MAC):
  - The “Group Address” field will display either a multicast group address (ASM or SSM) or the MAC address for the multicast group (MAC). In the examples for this command, the forwarding mode is changed to MAC to show how the “Group Address” field changes.
  - The “Host Address” field will display zero (MAC) or the IP host address for the bridge entry (ASM or SSM).

Examples

```
-> show ip multicast bridge-forward

Total 2 Bridge Entries

Vlan/Service  Type    Group Address     Host Address Next Interface UpTime
------------+-------+-----------------+-----------+--------------+--------------
vlan 1        asm     224.1.2.3                     1/4/12         00h:00m:01s
vlan 10       mac     01-00-5e-09-08-07             1/4/12         00h:00m:05s

-> show ip multicast bridge-forward vlan 10

Total 1 Bridge Entries

Vlan/Service  Type    Group Address     Host Address Next Interface UpTime
------------+-------+-----------------+-----------+--------------+--------------
vlan 10       mac     01-00-5e-09-08-07             1/4/12         00h:00m:05s
```

output definitions

Vlan/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast bridge entry.
Type	The bridge entry type (**asm**, **ssm**, **mac**). Configured through the **ip multicast forward-mode** command.
Group Address	If the bridge entry type is ASM or SSM, this field displays the destination IP group address; if the bridge entry type is MAC, this field displays the destination MAC address.
Host Address	The source IP host address (only applies to SSM bridge entries, otherwise this field is blank).
Next Interface	The destination interface for the bridge forwarding entry.
UpTime	The amount of time that has elapsed since the bridge forward entry was created.

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02: **service** parameter added.

Related Commands

show ip multicast bridge	Displays the IP multicast bridge table entries.

MIB Objects

```
alaIpmsBridgeForwardTable
   alaIpmsBridgeForwardConfigType,
   alaIpmsBridgeForwardAddressType,
   alaIpmsBridgeForwardValue,
   alaIpmsBridgeForwardType,
   alaIpmsBridgeForwardGroupAddress,
   alaIpmsBridgeForwardHostAddress,
   alaIpmsBridgeForwardNextIfIndex,
   alaIpmsBridgeForwardNextSubValue
   alaIpmsBridgeForwardUpTime
```

show ip multicast bidir-forward

Displays the IP multicast Bidirectional Protocol Independent Multicast (BIDIR-PIM) forwarding table entries for the specified IP multicast group address or all the entries if no IP multicast group address is specified.

show ip multicast bidir-forward [*ip_address***] [all-vrf]**

Syntax Definitions

ip_address	IP multicast group address.
all-vrf	Display forwarding table entries for all of the virtual routing and forwarding (VRF) instances.

Defaults

By default, BIDIR-PIM forwarding entries for all of the IP multicast groups are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 9900

Usage Guidelines

- Use the *ip_address* parameter to display BIDIR-PIM forwarding table entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the BIDIR-PIM forwarding table entries that exist in all of the VRF instances on the switch.

Examples

```
-> vrf vrf-1 show ip multicast bidir-forward

VRF:vrf-1  Total 2 Forwards

                  Egress
Group Address   Vlan/Service  Interface
---------------+-------------+-----------
225.0.1.0       vlan 30       1/2/1
                vlan 30       1/2/2

-> show ip multicast bidir-forward all-vrf

VRF:default  Total 3 Forwards

                  Egress
Group Address   Vlan/Service  Interface
---------------+-------------+-----------
225.0.1.0       vlan 20       1/1/1
                vlan 20       1/1/2
225.0.1.1       vlan 21       1/1/2
```

```
VRF:vrf-1  Total 2 Forwards

                  Egress
Group Address   Vlan/Service  Interface
--------------+-------------+-----------
225.0.1.0       vlan 30       1/2/1
                vlan 30       1/2/2
```

output definitions

VRF	The VRF instance for the BIDIR route.
Group Address	IP group address for the BIDIR route.
Egress VLAN/Service	The destination VLAN or Shortest Path Bridging (SPB) service for the BIDIR route.
Interface	Destination VLAN port or SPB virtual port for the BIDIR route.

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip multicast bridge-forward	Displays the forwarding state of the IP multicast bridge table entries.

MIB Objects

```
alaIpmsForwardTable
   alaIpmsBidirForwardAddressType
   alaIpmsBidirForwardGroupAddress
   alaIpmsBidirForwardType
   alaIpmsBidirForwardValue
   alaIpmsBidirForwardIfindex
   alaIpmsBidirForwardSubValue
```

show ip multicast profile

Displays a list of available IPMS configuration profiles or the parameter settings for a specific profile.

show ip multicast profile [*profile_name***]**

Syntax Definitions

profile_name	The name of an existing IPMS profile.

Defaults

By default, a list of available profiles is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The specified profile name must already exist in the switch configuration.

Examples

```
-> show ip multicast profile

Total 2 Profiles

Profile Name
--------------------------------
default
IGMPv3 with Zapping

-> show ip multicast profile "IGMPv3 with Zapping"

Status                                          = enabled,
Flood Unknown                                   = none,
Version                                         = 3,
Robustness                                      = 0,
Querying                                        = none,
Query Interval (seconds)                        = 0,
Query Response Interval (tenths of seconds)     = 0,
Last Member Query Interval (tenths of seconds)  = 0,
Unsolicited Report Interval (seconds)           = 0,
Proxying                                        = enabled,
Spoofing                                        = none,
Zapping                                         = enabled,
Querier Forwarding                              = none,
Router Timeout (seconds)                        = 0,
Source Timeout (seconds)                        = 0,
Max-group                                       = 0,
Max-group action                                = none,
Helper-address                                  = 0.0.0.0,
Static Querier Address                          = 0.0.0.0,
Static Spoofer Address                          = 0.0.0.0,
```

```
Zero-based Query                                = none,
Forward Mode                                    = none,
Update Delay Interval (milliseconds)            = 0,
SSM Mapping                                     = none,
Fast Join                                       = none,
Initial Packet Buffering                        = none,
    Max Flows                                   = 0,
    Max Packets Per Flow                        = 0,
    Buffer Timeout (seconds)                    = 0,
    Min Delay (milliseconds)                    = 0
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

ip multicast profile	Defines an IPMS profile that is used to apply a pre-defined IPMS configuration.
ip multicast apply-profile	Applies the specified IPMS profile to the specified IPMS instance.
show ip multicast	Displays the profile assignment for the IPMS instance.

MIB Objects

```
 alaIpmsProfileTable
   alaIpmsProfileAddressType
   alaIpmsProfileName
   alaIpmsProfileIndex
   alaIpmsProfileRowStatus
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigProfileNam
```

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

show ipv6 multicast [vlan *vlan_id* **| service** *service_id***]**

Syntax Definitions

vlan_id	VLAN for which to display the configuration.
service_id	SPB service ID number (1–32767). *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

By default, the status and general configuration parameters for the system are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify a VLAN ID to display the configuration information for a specific VLAN.
- Specify an SPB service ID to display the configuration information for a specific SPB service.

Examples

```
-> show ipv6 multicast

Profile                                          = default,
Status                                           = disabled,
Flood Unknown                                    = disabled,
Version                                          = 1,
Robustness                                       = 2,
Querying                                         = disabled,
Query Interval (seconds)                         = 125,
Query Response Interval (milliseconds)           = 10000,
Last Member Query Interval (milliseconds)        = 1000,
Unsolicited Report Interval (seconds)            = 1,
Proxying                                         = disabled,
Spoofing                                         = disabled,
Zapping                                          = disabled,
Querier Forwarding                               = disabled,
Router Timeout (seconds)                         = 90,
Source Timeout (seconds)                         = 30,
Max-group                                        = 0,
Max-group action                                 = none,
Helper-address                                   = ::,
Static Querier Address                           = ::,
Static Spoofer Address                           = ::,
```

```
Zero-based Query                                = enabled,
Forward Mode                                    = auto,
Update Delay Interval (milliseconds)            = 0,
SSM Mapping                                     = disabled,
Fast Join                                       = disabled,
Initial Packet Buffering                        = disabled,
    Max Flows                                   = 32,
    Max Packets Per Flow                        = 32,
    Buffer Timeout (seconds)                    = 10,
    Min Delay (milliseconds)                    = 0

-> show ipv6 multicast vlan 200

Profile                                         = default,
Status                                          = disabled,
Flood Unknown                                   = disabled,
Version                                         = 1,
Robustness                                      = 2,
Querying                                        = disabled,
Query Interval (seconds)                        = 125,
Query Response Interval (milliseconds)          = 10000,
Last Member Query Interval (milliseconds)       = 1000,
Unsolicited Report Interval (seconds)           = 1,
Proxying                                        = disabled,
Spoofing                                        = disabled,
Zapping                                         = disabled,
Querier Forwarding                              = disabled,
Router Timeout (seconds)                        = 90,
Source Timeout (seconds)                        = 30,
Max-group                                       = 0,
Max-group action                                = none,
Helper-address                                  = ::,
Static Querier Address                          = ::,
Static Spoofer Address                          = ::,
Zero-based Query                                = disabled,
Forward Mode                                    = auto,
Update Delay Interval (milliseconds)            = 0,
SSM Mapping                                     = disabled,
Fast Join                                       = disabled,
Initial Packet Buffering                        = disabled,
    Max Flows                                   = 32,
    Max Packets Per Flow                        = 32,
    Buffer Timeout (seconds)                    = 10,
    Min Delay (milliseconds)                    = 0

-> show ipv6 multicast service 20

Profile                                         = default,
Status                                          = disabled,
Flood Unknown                                   = disabled,
Version                                         = 1,
Robustness                                      = 2,
Querying                                        = disabled,
Query Interval (seconds)                        = 125,
Query Response Interval (milliseconds)          = 10000,
Last Member Query Interval (milliseconds)       = 1000,
Unsolicited Report Interval (seconds)           = 1,
Proxying                                        = disabled,
Spoofing                                        = disabled,
```

```
Zapping                                          = disabled,
Querier Forwarding                               = disabled,
Router Timeout (seconds)                         = 0,
Source Timeout (seconds)                         = 300,
Max-group                                        = 0,
Max-group action                                 = none,
Helper-address                                   = ::,
Static Querier Address                           = ::,
Static Spoofer Address                           = ::,
Zero-based Query                                 = disabled,
Forward Mode                                     = mac,
Update Delay Interval (milliseconds)             = 0,
SSM Mapping                                      = disabled,
Fast Join                                        = disabled,
Initial Packet Buffering                         = disabled,
    Max Flows                                    = 32,
    Max Packets Per Flow                         = 32,
    Buffer Timeout (seconds)                     = 10,
    Min Delay (milliseconds)                     = 0
```

output definitions

Profile	The name of a predefined IPMS configuration profile that is assigned to this instance. Configured through the **ipv6 multicast profile** command.
Status	Whether the IPv6 Multicast Switching and Routing is **Enabled** or **Disabled** (the default status).Configured through the **ipv6 multicast admin-state** command.
Flood Unknown	Whether the flooding of initial unknown multicast traffic is **Enabled** or **Disabled** (the default status). Configured through the **ipv6 multicast flood-unknown** command.
Version	Displays the default MLD version, which can be **1** or **2**. Configured through the **ipv6 multicast version** command.
Robustness	Displays the MLD robustness value, ranging from **1** to **7.** (The default value is 2). Configured through the **ipv6 multicast robustness** command.
Querying	Whether MLD querying is **Enabled** or **Disabled** (the default status). Configured through the **ipv6 multicast querying** command.
Query Interval (seconds)	Displays the time (in seconds) between MLD queries. (The default value is 125 seconds). Configured through the **ipv6 multicast query-interval** command.
Query Response Interval (milliseconds)	Displays the time (in milliseconds) taken to reply to an MLD query message. (The default value is 100 tenths-of-seconds). Configured through the **ipv6 multicast query-response-interval** command.
Last Member Query Interval (milliseconds)	Displays the time (in milliseconds) taken to reply to an MLD query message sent in response to a leave group message. (The default value is 10 tenths-of-seconds.) Configured through the **ipv6 multicast last-member-query-interval** command.
Unsolicited Report Interval (seconds)	Displays the time period (in seconds) to proxy any changed MLD membership state. (The default value is 1 second). Configured through the **ipv6 multicast unsolicited-report-interval** command.

output definitions

Proxying	Whether MLD proxying on the system is **Enabled** or **Disabled** (the default status)**.** Configured through the **ipv6 multicast proxying** command.
Spoofing	Whether MLD spoofing on the system is **Enabled** or **Disabled** (the default status)**.** Configured through the **ipv6 multicast spoofing** command.
Zapping	Whether MLD zapping on the system is **Enabled** or **Disabled** (the default status)**.** Configured through the **ipv6 multicast zapping** command.
Querier Forwarding	Whether MLD querier forwarding on the system is **Enabled** or **Disabled** (the default status)**.** Configured through the **ipv6 multicast querier-forwarding** command.
Router Timeout (seconds)	Displays the MLD router timeout in seconds. (The default value is 90 seconds.) Configured through the **ipv6 multicast router-timeout** command.
Source Timeout (seconds)	Displays the MLD source timeout in seconds. (The default value is 30 seconds.) Configured through the **ipv6 multicast source-timeout** command.
Max-group	Displays the global maximum group limit that can be learned per VLAN instance. (The default value is 0 which means no limit is imposed). Configured through the **ipv6 multicast max-group** command.
Max-group action	Displays the action taken when the maximum group limit has been exceeded, which can be **none**, **drop** or **replace**. Configured through the **ipv6 multicast max-group** command.
Helper-address	Displays the destination IPv6 address of a relay host, where MLD host reports and Leave messages are to be sent. (By default, no Helper-address is configured.) *This function is supported only in the VLAN domain; service domain is not supported.*
Static Querier Address	The Static Source IPv6 Address to be used when querying. (The default value of "::" indicates that this is not configured.) *This function is currently not supported.*
Static Spoofing Address	The Static Source IPv6 Address to be used when spoofing. (The default value of "::" indicates that this is not configured.) Configured through the **ipv6 multicast spoofing static-source-ip** command.
Zero-based Query	The current state of Zero-based Querying, which can be **disabled** or **enabled** (the default status). Configured through the **ipv6 multicast zero-based-query** command.
Forward Mode	Displays the current IPv6 Forwarding mode (**asm**, **ssm**, **mac**, or **auto**). Configured through the **ipv6 multicast forward-mode** command.
Update Delay Interval (milliseconds)	Displays the amount of time (in milliseconds) between propagating IPMS state changes. (The default value is 0 milliseconds). Configured through the **ipv6 multicast update-delay-interval** command.

output definitions

SSM Mapping	Whether Source Specific Multicast (SSM) mapping is **enabled** or **disabled** (the default). When enabled, Any Source Multicast (ASM) group memberships are translated into SSM group memberships. Configured through the **ipv6 multicast ssm-map** command. *This function is currently not supported.*
Fast Join	Whether the IP Multicast Switching fast join functionality is **enabled** or **disabled** (the default). When enabled, forwarding entries are automatically created in hardware as soon as group memberships are learned instead of waiting for the multicast traffic to reach the switch. Configured through the **ipv6 multicast fast-join** command.
Initial Packet Buffering	Whether Initial Packet Buffering is **enabled** or **disabled** (the default status). Configured through the **ipv6 multicast initial-packet-buffer admin-state** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Max Flows	The maximum number of IPv6 multicast flows buffered for initial packet. Configured through the **ipv6 multicast initial-packet-buffer max-flow** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Max Packets Per Flow	The maximum number of initial packets buffered per IPv6 multicast flow. Configured through the **ipv6 multicast initial-packet-buffer max-packet** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Buffer Timeout (seconds)	The timeout value for the initial buffered IPv6 multicast packets. Configured through the **ipv6 multicast initial-packet-buffer timeout** command. *This function is supported only in the VLAN domain; service domain is not supported.*
Min Delay (milliseconds)	The minimum delay to program the multicast replication index for IPv6 multicast flows buffered for initial packet. Configured through the **ipv6 multicast initial-packet-buffer min-delay** command. *This function is supported only in the VLAN domain; service domain is not supported.*

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; display fields added.
Release 8.4.1; **service** parameter added.

Related Commands

ipv6 multicast admin-state	Enables or disables IPv6 Multicast Switching and Routing on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigStatus
   alaIpmsConfigQuerying
   alaIpmsConfigProxying
   alaIpmsConfigSpoofing
   alaIpmsConfigZapping
   alaIpmsConfigQuerierForwarding
   alaIpmsConfigVersion
   alaIpmsConfigRobustness
   alaIpmsConfigQueryInterval
   alaIpmsConfigQueryResponseInterval
   alaIpmsConfigLastMemberQueryInterval
   alaIpmsConfigUnsolicitedReportInterval
   alaIpmsConfigRouterTimeout
   alaIpmsConfigSourceTimeout
   alaIpmsConfigMaxGroupLimit
   alaIpmsConfigMaxGroupExceedAction
   alaIpmsConfigFloodUnknown
   alaIpmsConfigMaxGroupLimit
   alaIpmsConfigMaxGroupExceedAction
   alaIpmsConfigHelperAddress
   alaIpmsConfigZeroBasedQuery
   alaIpmsConfigInitialPacketBuffer
   alaIpmsConfigDisplayInterfaceNames
   alaIpmsConfigUpdateDelayInterval
   alaIpmsConfigForwardMode
   alaIpmsConfigQueryingStaticSourceAddress
   alaIpmsConfigSpoofingStaticSourceAddress
```

show ipv6 multicast port

Displays the maximum group configuration applicable for the specified port or the specified Service Access Point (SAP) port. The current number of groups learned on a port, port/VLAN, SAP port, or SAP port/Shortest Path Bridging (SPB) service instance is also displayed.

show ipv6 multicast {port [*chassis/slot/port***] | sap port** [*sap_id*]}

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
sap_id	The SAP ID (chassis/slot/port:encapsulation).*This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify a port number to display the configuration information for a specific port.
- Specify a SAP ID to display the configuration information for a specific SAP port.
- When using the **sap port** parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ip multicast static-querier service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID).
- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

Examples

```
-> show ipv6 multicast port
Legends: Interface Max-group          = Max-group limit on the interface
         Interface Action             = Max-group action on the interface
         Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
         Interface-Instance Action    = Active Max-group action on the Lan Interface instance

Total 1 Lan Interface Instances

Interface      Vlan/Service Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
--------------+------------+-------+---------+---------+------------------+-----------------
1/4/38         vlan 1001    0       0         none      0                  none
1/5/43         vlan 1002    0       0         none      0                  none
1/6/23         vlan 1003    0       0         none      0                  none
```

```
-> show ipv6 multicast port 1/6/23

Legends: Interface Max-group          = Max-group limit on the interface
         Interface Action             = Max-group action on the interface
         Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
         Interface-Instance Action    = Active Max-group action on the Lan Interface instance

Total 1 Lan Interface Instances

Interface      Vlan/Service Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
---------------+------------+-------+---------+---------+------------------+------------------
1/6/23         vlan 1003    0       0         none      0                  none

-> show ipv6 multicast sap port

Legends: Interface Max-group          = Max-group limit on the interface
         Interface Action             = Max-group action on the interface
         Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
         Interface-Instance Action    = Active Max-group action on the Lan Interface instance

Total 1 Lan Interface Instances

Interface      Vlan/Service Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
---------------+------------+-------+---------+---------+------------------+------------------
sap:1/1/5:100  service 20   0       0         none      0                  none
sap:1/1/23:200 service 30   0       0         none      0                  none
sap:1/3/10:14  service 10   0       0         none      0                  none

-> show ipv6 multicast sap port 1/1/23:200

Legends: Interface Max-group          = Max-group limit on the interface
         Interface Action             = Max-group action on the interface
         Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
         Interface-Instance Action    = Active Max-group action on the Lan Interface instance

Total 1 Lan Interface Instances

Interface      Vlan/Service Current Interface Interface Interface-Instance Interface-Instance
                            Groups  Max-group Action    Max-group          Action
---------------+------------+-------+---------+---------+------------------+------------------
sap:1/1/23:200 service 30   0       0         none      0                  none
```

output definitions

Interface	The VLAN port or the SAP (chassis/slot/port:encapsulation) that serves as the virtual port for the SPB service.
Vlan/Service	The VLAN or SPB service ID associated with the IPv6 multicast interface.
Current Groups	The current groups associated with the IPv6 multicast interface.
Interface Max-group	The maximum group count allowed on the port or SAP port. This limit is applicable on the given port for all VLAN or service instances of the port.
Interface Action	The action to be taken when the group membership limit is exceeded (**none**, **drop**, or **replace**).

output definitions

Interface-Instance Max-group	The maximum group limit learned per port for the given VLAN or per SAP port for the given SPB service. This limit is applied to each port that is a member of the given VLAN or each SAP port that is a member of the given service.
Interface-Instance Action	The action to be taken when the group membership limit is exceeded (**none**, **drop**, or **replace**).

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **sap port** parameter added.

Related Commands

ipv6 multicast port max-group	Configures the maximum group limit learned per port.
ipv6 multicast max-group	Configures the maximum group limit learned per port for the specified VLAN, SPB service, or on the system if no VLAN or SPB service is specified.

MIB Objects

```
alaIpmsIntfStatsConfigType
   alaIpmsIntfStatsAddressType
   alaIpmsIntfStatsValue
   alaIpmsIntfStatsCurrentGroupCount
   alaIpmsIntfStatsMaxGroupLimit
   alaIpmsIntfStatsMaxGroupExceedAction
```

show ipv6 multicast forward

Display the IPv6 Multicast Switching and Routing forwarding table entries for the specified IPv6 multicast group address or all entries if no IPv6 multicast address is specified.

show ipv6 multicast forward [*ipv6_ddress***] [vlan [***vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

ipv6_address	IPv6 multicast group address.
vlan [*vlan_id***[-***vlan_id2***]**	Display forwarding table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display forwarding table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display forwarding table entries for all of the VRF instances.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ipv6_address* parameter to display forwarding entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the forwarding table entries that exist in all of the VRF instances on the switch.
- Forwarding entries are derived by applying the state from the source table to the state in the group, neighbor, and querier tables.
- On an OmniSwitch 9900, this command is available only when IP Multicast Switching *and* Routing is enabled for the switch. To view the multicast forwarding database on an OS6465 or OS6560 see the **show ipv6 multicast bridge** and **show ipv6 multicast bridge-forward** commands.
- Use the **ipv6 multicast display-interface-names** command to enable displaying the associated IPv6 interface name in the “Ingress Vlan/Service” and “Egress Vlan/Service” fields instead of the VLAN ID or service ID.

Examples

```
-> show ipv6 multicast forward

Total 3 Forwards
                                                  Ingress    Egress
Group Address   Host Address    Tunnel Address  VLAN/Service VLAN/Service Interface
---------------+---------------+---------------+------------+------------+---------
ff05::6         4444::2         ::               vlan 20      vlan 20      1/1/2
ff05::7         4444::2         ::               vlan 20      vlan 20      1/1/2
ff06::1         ::              ::               vlan 20      vlan 21      1/1/2

-> show ipv6 multicast forward ff05::6

Total 1 Forwards
                                                  Ingress    Egress
Group Address   Host Address    Tunnel Address  VLAN/Service VLAN/Service Interface
---------------+---------------+---------------+------------+------------+---------
ff05::6         4444::2         ::               vlan 20      vlan 20      1/1/2

-> show ipv6 multicast forward service

Total 3 Forwards
                                                  Ingress    Egress
Group Address   Host Address    Tunnel Address VLAN/Service VLAN/Service Interface
---------------+---------------+--------------+------------+------------+----------
ff05::6         4444::2         ::             service 10   service 10   sdp:32776
ff05::7         4444::2         ::             service 10   service 10   sdp:32776
ff06::1         ::              ::             service 10   service 10   sap:1/5:10

-> show ipv6 multicast forward vlan

Total 3 Forwards
                                                  Ingress            Egress
Group Address   Host Address    Tunnel Address  VLAN/Service VLAN/Service Interface
---------------+---------------+---------------+------------+------------+---------
ff05::6         4444::2         ::               vlan 20      vlan 20      1/1/2
ff05::7         4444::2         ::               vlan 20      vlan 20      1/1/2
ff06::1         ::              ::               vlan 20      vlan 21      1/1/2
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast forward vlan

Total 3 Forwards
                                                  Ingress            Egress
Group Address   Host Address    Tunnel Address  VLAN/Service VLAN/Service Interface
---------------+---------------+---------------+------------+------------+---------
ff05::6         4444::2         ::               VlanToLab    VlanToLab    1/1/2
ff05::7         4444::2         ::               VlanToLab    VlanToLab    1/1/2
ff06::1         ::              ::               VlanToCore   VlanToDist   1/1/2
```

output definitions

Group Address	IPv6 group address of the IPv6 multicast forward.
Host Address	IPv6 host address of the IPv6 multicast forward.
Tunnel Address	IPv6 source tunnel address of the IPv6 multicast forward.

output definitions (continued)

Ingress VLAN/Service	The ingress VLAN or Shortest Path Bridging (SPB) service ID associated with the IPv6 multicast forward. If the global display interface names option is enabled, then the ingress interface name associated with the IPv6 multicast forward is displayed.
Egress VLAN/Service	The egress VLAN or SPB service ID associated with the IPv6 multicast forward. If the global display interface names option is enabled, then the egress interface name associated with the IPv6 multicast forward is displayed. The egress interface (port) will also be included in the forward entry with both output formats.
Interface	The VLAN port or SPB virtual port of the IPv6 multicast forward.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

ipv6 multicast static-group	Creates a static MLD group entry on a specified port on a specified VLAN.

MIB Objects

```
alaIpmsForwardTable
  alaIpmsForwardConfigType
  alaIpmsForwardAddressType
  alaIpmsForwardValue
  alaIpmsForwardGroupAddress
  alaIpmsForwardHostAddress
  alaIpmsForwardDestAddress
  alaIpmsForwardOrigAddress
  alaIpmsForwardType
  alaIpmsForwardNextConfigType
  alaIpmsForwardNextValue
  alaIpmsForwardNextIfIndex
  alaIpmsForwardNextType
```

show ipv6 multicast neighbor

Displays the MLD neighbor table entries of IPv6 Multicast Switching and Routing.

show ipv6 multicast neighbor [vlan [*vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

vlan [*vlan_id***[-***vlan_id2***]**	Display MLD neighbor table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display MLD neighbor table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display MLD neighbor table entries for all of the VRF instances.

Defaults

By default, only the neighbor table entries specific to the current VRF instance are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **all-vrf** parameter option to display the IPv6 neighbor table entries that exist in all of the VRF instances on the switch.
- Interfaces with neighbors receive all IPv6 multicast, including all MLD traffic.
- Use the **ipv6 multicast display-interface-names** command to enable displaying the associated IPv6 interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ipv6 multicast neighbor

Total 4 Neighbors

Host Address               Vlan/Service   Interface            Static  Count  Life
--------------------------+-------------+--------------------+-------+------+-----
fe80::2a0:ccff:fed3:2853   vlan 20        1/1/2                no      1      6
fe80::2a0:ccff:fed3:2853   service 20     SAP:1/5:10           no      5520   172
::                         vlan 20        1/1/13               yes     0      0
::                         service 20     SAP:1/5:20           no      5520   172

-> show ipv6 multicast neighbor service

Total 2 Neighbors

Host Address               Vlan/Service   Interface            Static  Count  Life
--------------------------+-------------+--------------------+-------+------+-----
```

```
fe80::2a0:ccff:fed3:2853   service 20     SAP:1/5:10           no      5520   172
::                         service 20     SAP:1/5:20           no      5520   172

-> show ipv6 multicast neighbor vlan

Total 2 Neighbors

Host Address               Vlan/Service   Interface            Static  Count  Life
-------------------------+--------------+--------------------+-------+------+-----
fe80::2a0:ccff:fed3:2853   vlan 20        1/1/2                no      1      6
::                         vlan 20        1/1/13               yes     0      0
```

Sample output when the global display interface names option is enabled:

```
-> ipv6 multicast display-interface-names
-> show ipv6 multicast neighbor vlan

Total 2 Neighbors

Host Address               Vlan/Service   Interface            Static  Count  Life
-------------------------+--------------+--------------------+-------+------+-----
fe80::2a0:ccff:fed3:2853   VlanToLab      1/1/2                no      1      6
::                         VlanToLab      1/1/13               yes     0      0
```

output definitions

Host Address	The IPv6 address of the IPv6 multicast neighbor.
VLAN/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IPv6 multicast neighbor. If the global display interface names option is enabled, then the interface name associated with the IP multicast neighbor is displayed.
Interface	The VLAN port or the SPB virtual port of the IPv6 multicast neighbor.
Static	Whether it is a static MLD neighbor or not.
Count	Displays the count of the IPv6 multicast neighbor.
Life	The life time of the IPv6 multicast neighbor.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

ipv6 multicast static-neighbor	Creates a static MLD neighbor entry on a specified port on a specified VLAN.

MIB Objects

```
alaIpmsNeighborTable
   alaIpmsNeighborConfigType
   alaIpmsNeighborAddressType
   alaIpmsNeighborValue
   alaIpmsNeighborIfIndex
   alaIpmsNeighborHostAddress
   alaIpmsNeighborCount
   alaIpmsNeighborTimeout
   alaIpmsNeighborUpTime
alaIpmsStaticNeighborTable
   alaIpmsStaticNeighborConfigType
   alaIpmsStaticNeighborAddressType
   alaIpmsStaticNeighborValue
   alaIpmsStaticNeighborIfIndex
   alaIpmsStaticNeighborRowStatus
```

show ipv6 multicast querier

Displays the MLD querier table entries of IPv6 Multicast Switching and Routing.

show ipv6 multicast querier [vlan [*vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]]**

Syntax Definitions

vlan [*vlan_id***[-***vlan_id2***]**	Display MLD querier table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display MLD querier table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display querier table entries for all of the VRF instances.

Defaults

By default, only MLD querier entries specific to the current VRF instance are displayed

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **all-vrf** parameter option to display the MLD querier table entries that exist in all of the VRF instances on the switch.
- Interfaces with queriers receive all MLD traffic, and if querier forwarding is enabled, these interfaces will also receive all IPv6 multicast traffic.
- Use the **ipv6 multicast display-interface-names** command to enable displaying the associated IPv6 interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ipv6 multicast querier

Total 4 Queriers

Host Address               Vlan/Service   Interface           Static  Count  Life
--------------------------+--------------+-------------------+-------+------+-----
fe80::2a0:ccff:fed3:2853   vlan 20        1/1/2               no      1      6
fe80::2a0:ccff:fed3:2853   service 20     SAP:1/5:10          no      5520   172
::                         vlan 20        1/1/13              yes     0      0
::                         service 20     SAP:1/5:20          no      5520   172
```

```
-> show ipv6 multicast querier service

Total 2 Queriers

Host Address               Vlan/Service   Interface            Static  Count  Life
--------------------------+-------------+--------------------+-------+------+-----
fe80::2a0:ccff:fed3:2853   service 20     SAP:1/5:10           no      5520   172
::                         service 20     SAP:1/5:20           no      5520   172

-> show ipv6 multicast querier vlan

Total 2 Queriers

Host Address               Vlan/Service   Interface            Static  Count  Life
--------------------------+-------------+--------------------+-------+------+-----
fe80::2a0:ccff:fed3:2853   vlan 20        1/1/2                no      1      6
::                         vlan 20        1/1/13               yes     0      0
```

Sample output when the global display interface names option is enabled:

```
-> ipv6 multicast display-interface-names
-> show ipv6 multicast querier vlan

Total 2 Queriers

Host Address               Vlan/Service   Interface            Static  Count  Life
--------------------------+-------------+--------------------+-------+------+-----
fe80::2a0:ccff:fed3:2853   VlanToLab      1/1/2                no      1      6
::                         VlanToLab      1/1/13               yes     0      0
```

output definitions

Host Address	The IPv6 address of the IPv6 multicast querier.
VLAN/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast querier. If the global display interface names option is enabled, then the IPv6 interface name associated with the IPv6 multicast querier is displayed
Interface	The VLAN port or the SPB virtual port of the IPv6 multicast querier.
Static	Whether it is a static MLD neighbor or not.
Count	Displays the count of the IPv6 multicast querier.
Life	The life time of the IPv6 multicast querier.

Release History

Release 7.1.1; command was introduced
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

ipv6 multicast static-querier	Creates a static MLD querier entry on a specified port on a specified VLAN.

MIB Objects

```
alaIpmsQuerierTable
   alaIpmsQuerierConfigType
   alaIpmsQuerierAddressType
   alaIpmsQuerierValue
   alaIpmsQuerierIfIndex
   alaIpmsQuerierHostAddress
   alaIpmsQuerierCount
   alaIpmsQuerierTimeout
   alaIpmsQuerierUpTime
alaIpmsStaticQuerierTable
   alaIpmsStaticQuerierConfigType
   alaIpmsStaticQuerierAddressType
   alaIpmsStaticQuerierValue
   alaIpmsStaticQuerierIfIndex
   alaIpmsStaticQuerierRowStatus
```

show ipv6 multicast group

Displays the MLD group membership table entries of IPv6 Multicast Switching and Routing for the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

show ipv6 multicast group [*ipv6_ddress***] [vlan [***vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

ipv6_ddress	IPv6 multicast group address.
vlan [*vlan_id***[-***vlan_id2***]**	Display MLD group membership entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display MLD group membership entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display group membership entries for all of the VRF instances.

Defaults

By default, all IPv6 multicast groups are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ipv6_ddress* parameter to display entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the MLD group membership table entries that exist in all of the VRF instances on the switch.
- Use the **ipv6 multicast display-interface-names** command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ipv6 multicast group ff05::5

Group Address   Source Address Vlan/Service Interface Mode     Static Count  Life
---------------+--------------+------------+----------+--------+------+------+-----
ff05::5         ::             vlan 21      1/1/19     exclude  no     1      145
ff05::5         ::             service 20   SAP:1/5:10 exclude  no     5520   172
```

```
-> show ipv6 multicast group service

Total 3 Groups

Group Address  Source Address Vlan/Service Interface   Mode     Static Count  Life
--------------+--------------+------------+-----------+--------+------+------+-----
ff05::5         ::             service 20  SAP:1/5:10  exclude  no     5520   172
ff05::6         ::             service 20  SAP:1/5:20  exclude  no     5520   172
ff05::7         ::             service 20  sdp:32776   exclude  no     5520   172

-> show ipv6 multicast group vlan

Total 3 Groups

Group Address   Source Address  Vlan/Service Interface Mode     Static Count  Life
---------------+---------------+------------+---------+--------+------+------+-----
ff05::5         ::               vlan 21      1/1/19    exclude  no     100    145
ff05::6         ::               vlan 21      1/1/19    exclude  no     100    145
ff05::7         ::               vlan 21      1/1/19    exclude  no     101    145
ff05::8         ::               vlan 100     1/1/20    exclude  yes    0      0
ff05::9         ::               vlan 101     1/1/21    exclude  yes    0      0
```

Sample output when the global display interface names option is enabled:

```
-> ipv6 multicast display-interface-names
-> show ipv6 multicast group vlan

Total 3 Groups

Group Address   Source Address  Vlan/Service Interface Mode     Static Count  Life
---------------+---------------+------------+---------+--------+------+------+-----
ff05::5         ::               VlanToLab    1/1/19    exclude  no     100    145
ff05::6         ::               VlanToLab    1/1/19    exclude  no     100    145
ff05::7         ::               VlanToLab    1/1/19    exclude  no     101    145
ff05::8         ::               VlanToCore   1/1/20    exclude  yes    0      0
ff05::9         ::               VlanToDist   1/1/21    exclude  yes    0      0
```

output definitions

Group Address	IPv6 address of the IPv6 multicast group.
Source Address	IPv6 address of the IPv6 multicast source.
Vlan/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IPv6 multicast group. If the global display interface names option is enabled, then the IPv6 interface name associated with the IPv6 multicast group is displayed.
Interface	The VLAN port or the SPB virtual port on which the group membership was learned.
Mode	MLD source filter mode.
Static	Whether it is a static MLD group or not.
Count	Number of MLD membership requests made.
Life	Life time of the MLD group membership.

Release History

Release 7.1.1; command was introduced
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

ipv6 multicast static-group	Creates a static MLD group entry on a specified port for the specified VLAN or on the specified SPB virtual port for the specified SPB service.

MIB Objects

```
alaIpmsMemberTable
   alaIpmsMemberConfigType
   alaIpmsMemberAddressType
   alaIpmsMemberValue
   alaIpmsMemberIfIndex
   alaIpmsMemberGroupAddress
   alaIpmsMemberSourceAddress
   alaIpmsMemberMode
   alaIpmsMemberCount
   alaIpmsMemberTimeout
alaIpmsStaticMemberTable
   alaIpmsStaticMemberConfigType
   alaIpmsStaticMemberConfigAddressType
   alaIpmsStaticMemberValue
   alaIpmsStaticMemberIfIndex
   alaIpmsStaticMemberGroupAddress
   alaIpmsStaticMemberRowStatus
```

show ipv6 multicast source

Displays the IPv6 Multicast Switching and Routing source table entries matching the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

show ipv6 multicast source [*ipv6_ddress***] [vlan [***vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

ipv6_address	IPv6 multicast group address.
vlan [*vlan_id***[-***vlan_id2***]**	Display source table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display source table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Displays source table entries for all of the VRF instances.

Defaults

By default, all source table entries are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ipv6_ddress* parameter to display entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the MLD source table entries that exist in all of the VRF instances on the switch.
- On an OmniSwitch 9900, this command is available only when IP Multicast Switching *and* Routing is enabled for the switch. To view the multicast forwarding database on an OS6465 or OS6560 see the **show ip multicast bridge** and **show ip multicast bridge-forward** commands.
- Use the **ipv6 multicast display-interface-names** command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ipv6 multicast source

Total 8 Sources
                                      Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         ::              vlan 21
ff05::6         4444::2         ::              service 20
ff05::7         4444::2         ::              vlan 21
ff05::7         4444::2         ::              service 20
```

```
ff06::1         ::              ::              vlan 20
ff06::1         ::              ::              servuce 21
ff06::2         ::              ::              vlan 20
ff06::2         ::              ::              service 21

-> show ipv6 multicast source ff05::6

Total 2 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         ::              vlan 21
ff05::6         4444::2         ::              service 20

-> show ipv6 multicast source service

Total 4 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         ::              service 20
ff05::7         4444::2         ::              service 20
ff06::1         ::              ::              servuce 21
ff06::2         ::              ::              service 21

-> show ipv6 multicast source vlan

Total 4 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         ::              vlan 21
ff05::7         4444::2         ::              vlan 21
ff06::1         ::              ::              vlan 20
ff06::2         ::              ::              vlan 20
```

Sample output when the global display interface names option is enabled:

```
-> ipv6 multicast display-interface-names
-> show ipv6 multicast source vlan

Total 4 Sources

                                    Source        Ingress
Group Address   Host Address    Tunnel Address  VLAN/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         ::              VlanToLab
ff05::7         4444::2         ::              VlanToLab
ff06::1         ::              ::              VlanToCore
```

```
ff06::2          ::              ::              VlanToCore
```

output definitions

Group Address	IPv6 group address of the IPv6 multicast source.
Host Address	IPv6 host address of the IPv6 multicast source.
Source Tunnel Address	IPv6 source tunnel address of the IPv6 multicast source.
Ingress VLAN/Service	The ingress VLAN or Shortest Path Bridging (SPB) service ID number associated with the IP multicast source. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast source is displayed.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

Related Commands

show ipv6 multicast tunnel	Display the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

MIB Objects

```
alaIpmsSourceTable
   alaIpmsSourceConfigType
   alaIpmsSourceAddressType
   alaIpmsSourceValue
   alaIpmsSourceGroupAddress
   alaIpmsSourceHostAddress
   alaIpmsSourceDestAddress
   alaIpmsSourceOrigAddress
   alaIpmsSourceType
   alaIpmsSourceUpTime
```

show ipv6 multicast tunnel

Displays the IPv6 Multicast Switching and Routing tunneling table entries matching the specified IPv6 multicast group address, or all entries if no IPv6 multicast address is specified.

show ipv6 multicast tunnel [*ipv6_address***] [vlan [***vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***]] [all-vrf]**

Syntax Definitions

ipv6_address	IPv6 multicast group address.
vlan [*vlan_id***[-***vlan_id2***]**	Display tunneling table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Display tunneling table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6900-C32, or OmniSwitch 6900-V72.*
all-vrf	Display the IPv6 tunneling table entries for all of the VRF instances.

Defaults

By default, all IPv6 tunnel entries are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *ip_address* parameter to display the tunnel entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the IPv6 multicast tunnel entries that exist in all of the VRF instances on the switch.
- Use the **ipv6 multicast display-interface-names** command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ipv6 multicast tunnel

Total 4 Tunnels

                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         5555::3         vlan 21
ff05::6         4444::2         ::              service 20
ff05::7         4444::2         5555::3         vlan 21
ff05::7         4444::2         ::              service 20
```

```
-> show ipv6 multicast tunnel service

Total 2 Tunnels

                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         ::              service 20
ff05::7         4444::2         ::              service 20

-> show ipv6 multicast tunnel vlan

Total 2 Tunnels

                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         5555::3         vlan 21
ff05::7         4444::2         5555::3         vlan 21
```

Sample output when the global display interface names option is enabled:

```
-> ipv6 multicast display-interface-names
-> show ipv6 multicast tunnel vlan

Total 2 Tunnels

                                  Destination      Ingress
Group Address   Host Address    Tunnel Address  Vlan/Service
---------------+---------------+---------------+---------------
ff05::6         4444::2         5555::3         VlanToLab
ff05::7         4444::2         5555::3         VlanToLab
```

output definitions

Group Address	IPv6 group address of the IPv6 multicast tunnel.
Host Address	IPv6 host address of the IPv6 multicast tunnel.
DestinationTunnel Address	IPv6 source tunnel address of the IPv6 multicast tunnel.
Ingress Vlan/Service	VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast tunnel. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast tunnel is displayed.

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1.R02; **vlan** and **service** parameters added.

Related Commands

show ipv6 multicast source	Displays the IPv6 Multicast Switching and Routing source table entries matching the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified

MIB Objects

```
alaIpmsTunnelTable
   alaIpmsTunnelConfigType
   alaIpmsTunnelAddressType
   alaIpmsTunnelValue
   alaIpmsTunnelGroupAddress
   alaIpmsTunnelHostAddress
   alaIpmsTunnelDestAddress
   alaIpmsTunnelOrigAddress
   alaIpmsTunnelType
   alaIpmsTunnelNextDestAddress
   alaIpmsTunnelNextType
```

show ipv6 multicast host-list

Displays the IPv6 multicast host address list configuration for the switch.

show ipv6 multicast host-list [*host_list_name***]**

Syntax Definitions

host_list_name	The name of an existing IPv6 multicast host list.

Defaults

By default, all host lists configured on the switch are displayed.

Platforms Supported

Not supported in this release.

Usage Guidelines

Use the *host_list_name* parameter to display information for a specific host list.

Examples

```
-> show ipv6 multicast host-list

Total 2 Lists

Host List Name                   Addresses
---------------------------------+---------------
group-map1                       3333::2
                                 3333::3
                                 3333::4
ssm-map1                         4444::2
                                 4444::3
                                 4444::4

-> show ipv6 multicast host-list ssm-map1

Host List Name                   Addresses
---------------------------------+---------------
ssm-map1                         4444::2
                                 4444::3
                                 4444::4
```

Release History

Release 8.3.1.R02; command introduced.

Related Commands

ipv6 multicast host-list	Configures a list of host IPv6 addresses that is used for IPv6 multicast group maps and SSM maps.

MIB Objects

```
alaIpmsHostListTable
   alaIpmsHostListName
   alaIpmsHostListAddressType
   alaIpmsHostListAddress
```

show ipv6 multicast ssm-map

Displays the IPv6 Source Specific Multicast (SSM) mapping configuration for the switch.

show ipv6 multicast ssm-map [vlan *vlan_id***]**

Syntax Definitions

vlan_id	VLAN for which to display the configuration.

Defaults

By default, all IPv6 multicast SSM mappings configured on the switch are displayed.

Platforms Supported

Not supported in this release.

Usage Guidelines

Specify a VLAN ID to display the configuration information for a specific VLAN.

Examples

```
-> show ipv6 multicast ssm-map
Type    Id    Group Address/Prefix  Source List Name
-------+-----+---------------------+-------------------------------
global  0     ff05::5/128           h-list1
vlan    200   ff05::6/128           h-list2

-> show ipv6 multicast ssm-map vlan 200
Type    Id    Group Address/Prefix  Source List Name
-------+-----+---------------------+-------------------------------
vlan    200   ff05::6/128           h-list2
```

Release History

Release 8.3.1.R02; command introduced.

Related Commands

ipv6 multicast ssm-map	Configures a list of host IP addresses that is used for IP multicast group maps and SSM maps.

MIB Objects

```
alaIpmsSsmMapTable
   alaIpmsSsmMapConfigType
   alaIpmsSsmMapConfigAddressType
   alaIpmsSsmMapConfigValue
   alaIpmsSsmMapGroupAddress
   alaIpmsSsmMapGroupPrefixLength
   alaIpmsSsmMapSourceListName
```

show ipv6 multicast bridge

Displays the IPv6 multicast bridge table entries that match the specified VLAN, Shortest Path Bridging (SPB) service, IPv6 multicast group address, MAC address, or all entries if no additional parameters are specified.

show ipv6 multicast bridge [vlan *vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***] |** *ipv6_address* **|** *mac_address***] [all-vrf]**

Syntax Definitions

vlan [*vlan_id***[-***vlan_id2***]**	Displays bridge table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Displays bridge table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465 or OmniSwitch 6560*
ipv6_address	IPv6 multicast group address.
mac_address	Group MAC address.
all-vrf	Display bridge table entries for all of the VRF instances.

Defaults

By default, all bridge table entries are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6465, 6560, 9900

Usage Guidelines

- Use one of the optional parameters (*vlan_id*, *service-id*, *ipv6_address*, *mac_address*) to display bridge table entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the source table entries that exist in all of the VRF instances on the switch.
- Based on the forwarding mode set for the switch (ASM, SSM, or MAC):
  - The “Group Address” field will display either a multicast group address (ASM or SSM) or the MAC address for the multicast group (MAC).
  - The “Host Address” field will display zero (MAC) or the IPv6 host address for the bridge entry (ASM or SSM).

Examples

```
-> show ipv6 multicast bridge vlan 130

Total 2 Bridge Entries

Vlan/Service   Type         Group Address     Host Address  Action      UpTime
--------------+------------+-----------------+-------------+-----------+-----------
vlan 130       asm          ff05::6                         forwarding  00h:00m:04s
service 10     mac          33-33-00-01-01-01               flooding    00h:00m:05s
```

output definitions

Vlan/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast bridge entry.
Type	The bridge type for the IPv6 multicast bridge entry (**asm**, **ssm**, **mac**). Configured through the **ipv6 multicast forward-mode** command.
Group Address	If the bridge entry type is ASM or SSM, this field displays the destination IP group address; if the bridge entry type is MAC, this field displays the destination MAC address.
Host Address	The source IPv6 host address (only applies to SSM bridge entries, otherwise this field is blank).
Action	The current action taken for the bridge entry (**forwarding** or **filtering**).
UpTime	The amount of time that has elapsed since the bridge entry was created.

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ipv6 multicast bridge-forward	Displays the forwarding state of the IPv6 multicast bridge table entries.

MIB Objects

```
alaIpmsBridgeTable
   alaIpmsBridgeConfigType
   alaIpmsBridgeAddressType
   alaIpmsBridgeValue
   alaIpmsBridgeType
   alaIpmsBridgeGroupAddress
   alaIpmsBridgeHostAddress
   alaIpmsBridgeUpTime
   alaIpmsBridgeAction
```

show ipv6 multicast bridge-forward

Displays the forwarding state of the IPv6 multicast bridge table entries that match the specified VLAN, Shortest Path Bridging (SPB) service, IPv6 multicast group address, MAC address, or all entries if no additional parameters are specified.

show ipv6 multicast bridge-forward [vlan *vlan_id***[-***vlan_id2***] | service [***service_id***[-***service_id2***] |** *ipv6_address* **|** *mac_address***] [all-vrf]**

Syntax Definitions

vlan [*vlan_id***[-***vlan_id2***]**	Displays bridge table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
service [*service_id***[-***service_id2***]**	Displays bridge table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is currently not supported on an OmniSwitch 6465 and OmniSwitch 6560.*
ipv6_address	IPv6 multicast group address.
mac_address	Group MAC address.
all-vrf	Display bridge table entries for all of the VRF instances.

Defaults

By default, all bridge table entries are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 6465, 6560, 9900

Usage Guidelines

- Use one of the optional parameters (*vlan_id*, *service_id*, *ipv6_address*, *mac_address*) to display forwarding information for a specific multicast group.
- Use the **all-vrf** parameter option to display the source table entries that exist in all of the VRF instances on the switch.
- Based on the forwarding mode set for the switch (ASM, SSM, or MAC):
  - The “Group Address” field will display either a multicast group address (ASM or SSM) or the MAC address for the multicast group (MAC). In the examples for this command, the forwarding mode is changed to MAC to show how the “Group Address” field changes.
  - The “Host Address” field will display zero (MAC) or the IPv6 host address for the bridge entry (ASM or SSM).

Examples

```
-> show ipv6 multicast bridge-forward vlan 130

Total 2 Bridge Forwarding Entries

Vlan/Service  Type        Group Address    Host Address Next Interface UpTime
------------+-----------+----------------+-----------+--------------+-----------
vlan 1        asm-partial ::1.1.2.3                     1/4/12         00h:00m:10s
vlan 130      asm         33-33-ff-ff-ff-ff             1/4/12         00h:00m:07s

-> ipv6 multicast vlan 130 forward-mode mac
-> show ipv6 multicast bridge-forward vlan 130

Total 1 Bridge Forwarding Entries

Vlan/Service  Type        Group Address    Host Address Next Interface UpTime
------------+-----------+----------------+-----------+--------------+-----------
vlan 130      mac         33-33-ff-ff-ff-ff             1/3/25         00h:00m:07s
```

output definitions

Vlan/Service	The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast bridge entry.
Type	The bridge entry type (**asm**, **ssm**, **mac**). Configured through the **ipv6 multicast forward-mode** command.
Group Address	If the bridge entry type is ASM or SSM, this field displays the destination IPv6 group address; if the bridge entry type is MAC, this field displays the destination MAC address.
Host Address	The source IPv6 host address (only applies to SSM bridge entries, otherwise this field is blank).
Next Interface	The destination interface for the bridge forwarding entry.
UpTime	The amount of time that has elapsed since the bridge forward entry was created.

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; **service** parameter added.

Related Commands

show ipv6 multicast bridge	Displays the IPv6 multicast bridge table entries.

MIB Objects

```
alaIpmsBridgeForwardTable
   alaIpmsBridgeForwardConfigType,
   alaIpmsBridgeForwardAddressType,
   alaIpmsBridgeForwardValue,
   alaIpmsBridgeForwardType,
   alaIpmsBridgeForwardGroupAddress,
   alaIpmsBridgeForwardHostAddress,
   alaIpmsBridgeForwardNextIfIndex,
   alaIpmsBridgeForwardNextSubValue
   alaIpmsBridgeForwardUpTime
```

show ipv6 multicast bidir-forward

Displays the IPv6 multicast Bidirectional Protocol Independent Multicast (BIDIR-PIM) forwarding table entries for the specified IPv6 multicast group address or all the entries if no IPv6 multicast group address is specified.

show ipv6 multicast bidir-forward [*ipv6_address***] [all-vrf]**

Syntax Definitions

ipv6_address	IPv6 multicast group address.
all-vrf	Display forwarding table entries for all of the VRF instances.

Defaults

By default, BIDIR-PIM forwarding entries for all of the IPv6 multicast groups are displayed for the current VRF instance.

Platforms Supported

OmniSwitch 9900

Usage Guidelines

- Use the *ipv6_address* parameter to display BIDIR-PIM forwarding table entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the BIDIR-PIM forwarding table entries that exist in all of the VRF instances on the switch.
- Use the **ipv6 multicast display-interface-names** command to enable displaying the associated IPv6 interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> vrf vrf-1 show ipv6 multicast bidir-forward

VRF:vrf-1   Total 3 Forwards

                  Egress
Group Address   Vlan/Service   Interface
---------------+--------------+-----------
ff05::6         vlan 30        1/2/1
                vlan 30        1/2/2
ff05::8         vlan 31        1/2/2
```

```
-> show ipv6 multicast bidir-forward all-vrf

VRF:default   Total 3 Forwards

                  Egress
Group Address   Vlan/Service   Interface
---------------+--------------+-----------
ff05::6         vlan 20        1/1/1
                vlan 20        1/1/2
ff05::8         vlan 21        1/1/2

VRF:vrf-1   Total 3 Forwards

                  Egress
Group Address   Vlan/Service   Interface
---------------+--------------+-----------
ff05::6         vlan 30        1/2/1
                vlan 30        1/2/2
ff05::8         vlan 31        1/2/2
```

Sample output when the global display interface names option is enabled:

```
-> ipv6 multicast display-interface-names
-> vrf vrf-1 show ipv6 multicast bidir-forward

VRF:vrf-1   Total 3 Forwards

                  Egress
Group Address   Vlan/Service   Interface
---------------+--------------+-----------
ff05::6         IPv6ToCore2    1/2/1
                IPv6ToCore2    1/2/2
ff05::8         IPv6ToLab2     1/2/2

-> show ipv6 multicast bidir-forward all-vrf

VRF:default   Total 3 Forwards

                  Egress
Group Address   Vlan/Service   Interface
---------------+--------------+-----------
ff05::6         vlanToCore     1/1/1
                vlanToCore1    1/1/2
ff05::8         vlanToLab1     1/1/2

VRF:vrf-1   Total 3 Forwards

                    Egress
Group Address   Vlan/Service   Interface
---------------+--------------+-----------
ff05::6         IPv6ToCore2    1/2/1
                IPv6ToCore2    1/2/2
ff05::8         IPv6ToLab2     1/2/2
```

output definitions

VRF	The VRF instance for the BIDIR route.
Group Address	IPv6 group address for the BIDIR route.

output definitions (continued)

Egress VLAN/Service	The destination VLAN or Shortest Path Bridging (SPB) service for the BIDIR route. If the global display interface names option is enabled, then the IPv6 interface name associated with the BIDIR route is displayed.
Interface	Destination VLAN port or SPB virtual port for the BIDIR route.

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ipv6 multicast bridge-forward	Displays the forwarding state of the IPv6 multicast bridge table entries.

MIB Objects

```
alaIpmsForwardTable
   alaIpmsForwardConfigType
   alaIpmsForwardAddressType
   alaIpmsForwardValue
   alaIpmsForwardGroupAddress
   alaIpmsForwardHostAddress
   alaIpmsForwardDestAddress
   alaIpmsForwardOrigAddress
   alaIpmsForwardType
   alaIpmsForwardNextConfigType
   alaIpmsForwardNextValue
   alaIpmsForwardNextIfIndex
   alaIpmsForwardNextType
```

show ipv6 multicast profile

Displays a list of available IPMS configuration profiles or the parameter settings for a specific profile.

show ipv6 multicast profile [*profile_name***]**

Syntax Definitions

profile_name	The name of an existing IPMS profile.

Defaults

By default, a list of available profiles is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The specified profile name must already exist in the switch configuration.

Examples

```
-> show ipv6 multicast profile

Total 2 Profiles

Profile Name
--------------------------------
default
IGMPv3 with Zapping

-> show ip multicast profile "IGMPv3 with Zapping"

Status                                          = enabled,
Flood Unknown                                   = none,
Version                                         = 3,
Robustness                                      = 0,
Querying                                        = none,
Query Interval (seconds)                        = 0,
Query Response Interval (tenths of seconds)     = 0,
Last Member Query Interval (tenths of seconds)  = 0,
Unsolicited Report Interval (seconds)           = 0,
Proxying                                        = enabled,
Spoofing                                        = none,
Zapping                                         = enabled,
Querier Forwarding                              = none,
Router Timeout (seconds)                        = 0,
Source Timeout (seconds)                        = 0,
Max-group                                       = 0,
Max-group action                                = none,
Helper-address                                  = ::,
Static Querier Address                          = ::,
Static Spoofer Address                          = ::,
```

```
Zero-based Query                                = none,
Forward Mode                                    = none,
Update Delay Interval (milliseconds)            = 0,
SSM Mapping                                     = none,
Fast Join                                       = none,
Initial Packet Buffering                        = none,
    Max Flows                                   = 0,
    Max Packets Per Flow                        = 0,
    Buffer Timeout (seconds)                    = 0,
    Min Delay (milliseconds)                    = 0
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

ipv6 multicast profile	Defines an IPMS profile that is used to apply a pre-defined IPMS configuration.
ipv6 multicast apply-profile	Applies the specified IPMS profile to the specified IPMS instance.
show ipv6 multicast	Displays the profile assignment for the IPMS instance.

MIB Objects

```
 alaIpmsProfileTable
   alaIpmsProfileAddressType
   alaIpmsProfileName
   alaIpmsProfileIndex
   alaIpmsProfileRowStatus
alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigProfileNam
```

32 DVMRP Commands

This chapter includes CLI command descriptions for Distance Vector Multicast Routing Protocol (DVMRP), version 3.

DVMRPv3 is a dense-mode multicast routing protocol that enables routers to efficiently propagate IP multicast traffic through a network. Multicast traffic consists of a data stream that originates from a single source and is sent to hosts that have subscribed to that stream. Live video broadcasts, video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news services are examples of multicast traffic.

For more information about configuring DVMRP, see the applicable *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide*.

MIB information for the DVMRP commands is as follows:

Filename: ALCATEL-IND1-VIRTUALROUTER-MIB.mib
Module: alcatelIND1VirtualRouterMIB

Filename: ALCATEL-IND1-DVMRP-MIB.mib
Module: alcatelIND1DVMRPMIB

Filename: DVMRP-STD-MIB.mib
Module: dvmrpStdMIB

A summary of the available commands is listed here:

ip load dvmrp

Dynamically loads DVMRP to memory.

ip load dvmrp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

This command must be executed before DVMRP can be configured on the switch. In addition, DVMRP must be administratively enabled before you can run the protocol on the switch. For more information, refer to the **ip dvmrp admin-state** command on page 32-3.

Examples

```
-> ip load dvmrp
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp admin-state	Globally enables or disables DVMRP protocol on the switch.

MIB Objects

```
alaVrConfigTable
   alaVrConfigDvmrpStatus
```

ip dvmrp admin-state

Globally enables or disables DVMRP protocol on the switch.

ip dvmrp admin-state {enable | disable}

Syntax Definitions

enable	Administratively enables DVMRP on the switch.
disable	Administratively disables DVMRP on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- This command must be set to **enable** before DVMRP can run on the switch. In addition, the **ip load dvmrp** command must be issued. For more information, refer to the **ip load dvmrp** command on page 32-2.
- To enable or disable DVMRP for a particular interface, refer to the **ip dvmrp interface** command on page 32-6.

Examples

```
-> ip dvmrp admin-state enable
-> ip dvmrp admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp interface	Enables or disables the DVMRP protocol on a specified interface.
ip load dvmrp	Dynamically loads DVMRP to memory.
show ip dvmrp	Displays global DVMRP parameters, including current status.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpAdminStatus
```

ip dvmrp flash-interval

Configures the minimum flash update interval value. The flash update interval defines how often routing table change messages are sent to neighboring DVMRP routers.

ip dvmrp flash-interval *seconds*

Syntax Definitions

seconds	Specifies the interval value, in seconds (5–86400).

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

Because routing table change messages are sent between the transmission of complete routing tables, the flash update interval value must be lower than the route report interval.

Examples

```
-> ip dvmrp flash-interval 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip dvmrp	Displays global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpFlashUpdateInterval
```

ip dvmrp graft-timeout

Configures the graft message retransmission value. The graft message retransmission value is the duration of time that the routing switch will wait before retransmitting a graft message if it has not received an acknowledgement from its neighbor.

ip dvmrp graft-timeout *seconds*

Syntax Definitions

seconds	Specifies the graft message retransmission value, in seconds (5–86400).

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp graft-timeout 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip dvmrp	Displays global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpGraftRetransmission
```

ip dvmrp interface

Enables or disables the DVMRP protocol on a specified interface.

ip dvmrp interface {*interface_name***}**

no ip dvmrp interface {*interface_name***}**

Syntax Definitions

interface_name	The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

Use the **no** form of this command to delete an interface.

Examples

```
-> ip dvmrp interface vlan-10
-> no ip dvmrp interface vlan-10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp admin-state	Globally enables or disables the DVMRP protocol on the switch.
ip dvmrp interface metric	Configures the distance metric for an interface, which is used to calculate distance vectors.
show ip dvmrp interface	Displays information for all multicast-capable interfaces.

MIB Objects

```
dvmrpInterfaceTable
   dvmrpInterfaceLocalAddress
   dvmrpInterfaceStatus
```

ip dvmrp interface metric

Configures the distance metric for an interface, which is used to calculate distance vectors. DVMRP uses the distance metric value to determine the most cost-effective way to pass data through the network.

ip dvmrp interface *interface_name* **metric** *value*

Syntax Definitions

interface_name	The name of the interface.
value	Specifies the metric value (1–31).

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

DVMRP uses the distance metric value to determine the most cost-effective way to pass data through the network. The higher the distance metric value, the higher the cost.

Examples

```
-> ip dvmrp interface vlan-2 metric 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp interface	Enables or disables the DVMRP protocol on a specified interface.
show ip dvmrp interface	Displays the DVMRP interface table.

MIB Objects

```
dvmrpInterfaceTable
   dvmrpInterfaceLocalAddress
   dvmrpInterfaceMetric
```

ip dvmrp interface mbr-default-information

Configures a DVMRP interface to advertise the default route for the interface. This command only applies when the local switch is operating in the Multicast Border Router (MBR) mode.

ip dvmrp interface *interface_name* **mbr-default-information {enable | disable}**

Syntax Definitions

interface_name	The name of the interface.
enable	Enables advertisement of the default route on the specified interface.
disable	Disables advertisement of the default route on the specified interface.

Defaults

By default, advertising the default route is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Advertising a default route on the DVMRP interface provides a method for ensuring that sources inside the PIM domain can reach all routers inside the DVMRP domain.
- Make sure that the default route is not advertised on the MBONE.

Examples

```
-> ip dvmrp interface mbr-default-information enable
-> ip dvmrp interface mbr-default-information disable
```

Release History

Release 7.3.2; command was introduced.

Related Commands

ip dvmrp interface	Enables or disables the DVMRP protocol on a specified interface.
show ip dvmrp interface	Displays the DVMRP interface table.

MIB Objects

```
alaDvmrpIfAugTable
   alaDvmrpIfMbrDefaultInfoStatus
```

ip dvmrp neighbor-interval

Configures the neighbor probe interval time. The neighbor probe interval time specifies how often probes are transmitted on DVMRP-enabled interfaces.

ip dvmrp neighbor-interval *seconds*

Syntax Definitions

seconds	Specifies the probe interval time, in seconds (5–30).

Defaults

parameter	default
seconds	10

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp neighbor-interval 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp neighbor-timeout	Configures the neighbor timeout.
show ip dvmrp neighbor	Displays the DVMRP neighbor table.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpNeighborProbeInterval
```

ip dvmrp neighbor-timeout

Configures the neighbor timeout. This value specifies how long the switch will wait for activity from a neighboring DVMRP router before assuming that the inactive router is down.

ip dvmrp neighbor-timeout *seconds*

Syntax Definitions

seconds	Specifies the neighbor timeout, in seconds (5–86400).

Defaults

parameter	default
seconds	35

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp neighbor-timeout 35
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp neighbor-interval	Configures the neighbor probe interval time.
show ip dvmrp neighbor	Displays the DVMRP neighbor table.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpNeighborTimeout
```

ip dvmrp prune-lifetime

Indicates the length of time a prune will be in effect—i.e., its *lifetime*. When the prune lifetime expires, the interface is joined back onto the multicast delivery tree. If unwanted multicast datagrams continue to arrive, the prune mechanism will be re-initiated and the cycle will continue.

ip dvmrp prune-lifetime *seconds*

Syntax Definitions

seconds	Specifies the prune lifetime, in seconds (180–86400).

Defaults

parameter	default
seconds	7200

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp prune-lifetime 7200
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp prune-timeout	Configures the prune packet retransmission value.
show ip dvmrp prune	Displays DVMRP prune entries, including the router's upstream prune state.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpPruneLifetime
```

ip dvmrp prune-timeout

Configures the prune packet retransmission value. This value is the duration of time that the routing switch will wait if it continues to receive unwanted multicast traffic before retransmitting a prune message.

ip dvmrp prune-timeout *seconds*

Syntax Definitions

seconds	Specifies retransmission time, in seconds (30–86400).

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp prune-timeout 30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp prune-lifetime	Indicates the length of time a prune will be in effect.
show ip dvmrp prune	Displays DVMRP prune entries, including the router's upstream prune state.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpPruneRetransmission
```

ip dvmrp report-interval

Configures the route report interval. This value defines how often the switch will send its complete routing table to neighboring routers running DVMRP.

ip dvmrp report-interval *seconds*

Syntax Definitions

seconds	Specifies the report interval, in seconds (10–2000).

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp report-interval 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip dvmrp route	Displays the DVMRP routes that are being advertised to other routers.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpRouteReportInterval
```

ip dvmrp route-holddown

Configures the time during which DVMRP routes are kept in a hold down state. A holddown state refers to the time that a route to an inactive network continues to be advertised.

ip dvmrp route-holddown *seconds*

Syntax Definitions

seconds	Specifies the holddown time, in seconds (1–86400).

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp route-holddown 120
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp route-timeout	Configures the route expiration timeout value.
show ip dvmrp	Displays the global DVMRP parameters.
show ip dvmrp route	Displays the DVMRP routes that are being advertised to other routers.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpRouteHoldDown
```

ip dvmrp route-timeout

Configures the route expiration timeout value. The route expiration timeout value specifies how long the switch will wait before aging out a route. When the route expiration timeout expires, the route is advertised as being in holddown until either its activity resumes or it is deleted from the route table.

ip dvmrp route-timeout *seconds*

Syntax Definitions

seconds	Specifies the timeout value, in seconds (20–4000).

Defaults

parameter	default
seconds	140

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp route-timeout 140
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp route-holddown	Configures the time during which DVMRP routes are kept in a hold down state.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpRouteExpirationTimeout
```

ip dvmrp subord-default

Changes the initial default assumption on a neighbor's subordinate or non-subordinate status. When the status value is true, DVMRP neighbors are assumed to be subordinate and traffic is automatically forwarded to the neighbor upon initial discovery. When the value is false, traffic is not forwarded to the neighbor until route reports have been exchanged and the neighbor has explicitly expressed dependency.

ip dvmrp subord-default {true | false}

Syntax Definitions

true	DVMRP neighbors are assumed subordinate; traffic is automatically forwarded to the neighbor on initial discovery.
false	DVMRP neighbors are *not* assumed to be subordinate; traffic is not forwarded until route reports have been exchanged and the neighbor has explicitly expressed dependency.

Defaults

parameter	default
true | false	**true**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- However, if neighbors in the DVMRP domain have difficulty handling large initial bursts of traffic, it is recommended that the neighbor's default status as a suboridinate be changed to false.
- To view the current subordinate neighbor status, use the **show ip dvmrp** command.

Examples

```
-> ip dvmrp subord-default false
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig
   alaDvmrpInitNbrAsSubord
```

show ip dvmrp

Displays the global DVMRP parameters configuration.

show ip dvmrp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> show ip dvmrp
DVMRP Admin Status          = enabled,
Flash Interval              = 5,
Graft Timeout               = 5,
Neighbor Interval           = 10,
Neighbor Timeout            = 35,
Prune Lifetime              = 7200,
Prune Timeout               = 30,
Report Interval             = 60,
Route Holddown              = 120,
Route Timeout               = 140,
Subord Default              = true,
BFD status                  = disabled,
MBR Operational Status      = enabled,

Number of Routes            = 3,
Number of Reachable Routes  = 3
```

output definitions

DVMRP Admin Status	The current global (i.e., switch-wide) status of DVMRP, which can be **enabled** or **disabled**. To change the current DVMRP global status, use the **ip dvmrp admin-state** command.
Flash Interval	The current minimum flash update interval value, in seconds. The flash interval defines how often routing table change messages are sent to neighboring DVMRP routers. Because routing table change messages are sent between the transmission of complete routing tables, the flash update interval must be shorter than the route report interval. The default value is 5.

output definitions (continued)

Graft Timeout	The graft message retransmission value, in seconds. The graft message retransmission value defines the duration of time that the routing switch will wait before retransmitting a graft message if it has not received an acknowledgement from its neighbor. Valid range from 5–86400. The default value is 5.
Neighbor Interval	The current neighbor probe interval time, in seconds. The neighbor probe interval time specifies how often probes are transmitted to interfaces with attached DVMRP neighbors. Valid range from 5–30. The default value is 10.
Neighbor Timeout	The current neighbor timeout value, in seconds. This value specifies how long the routing switch will wait for activity from a neighboring DVMRP router before assuming the inactive router is down. Valid range from 5–86400. The default value is 35.
Prune Lifetime	The length of time, in seconds, a prune will be in effect. When the prune lifetime expires, the interface is joined back onto the multicast delivery tree. If unwanted multicast datagrams continue to arrive, the prune mechanism will be re-initiated and the cycle will continue. Valid range from 180–86400. The default value is 7200.
Prune Timeout	The current prune packet retransmission value, in seconds. This value indicates the duration of time that the routing switch will wait if it continues to receive unwanted multicast traffic before retransmitting a prune message. Valid range from 30–86400. The default value is 30.
Report Interval	The current route report interval, in seconds. The route report interval defines how often routers will send their complete routing tables to neighboring routers running DVMRP. Valid range from 10–2000. The default value is 60.
Route Holddown	The current holddown time, in seconds. This value indicates the time during which DVMRP routes are kept in a holddown state. A holddown state refers to the time that a route to an inactive network continues to be advertised. Valid range from 1–120. The default value is 120.
Route Timeout	The current route expiration timeout value, in seconds. The route expiration timeout value specifies how long the routing switch will wait before aging out a route. Valid range from 20–4000. The default value is 140.
Subord Default	Displays the initial default assumption on a neighbor's subordinate or non-subordinate status. When the status value is true, DVMRP neighbors are assumed to be subordinate and traffic is automatically forwarded to the neighbor upon initial discovery. When the value is false, traffic is not forwarded to the neighbor until route reports have been exchanged and the neighbor has explicitly expressed dependency. To change the current subordinate neighbor status, use the **ip dvmrp subord-default** command. Options include **true** and **false**. The default value is true.
BFD Status	Not supported in the current release.
MBR Operational Status	Indicates whether or not DVMRP interaction with PIM is **enabled** or **disabled** on a MBR switch. MBR functionality is not operationally active until both PIM and DVMRP have at least one enabled and active interface.

output definitions (continued)

Number of Routes	The number of entries in the routing table. This number can be used to monitor the routing table size and detect illegal advertisements of unicast routes.
Number of Reachable Routes	The total number of reachable routes. The number of entries in the routing table with non-infinite metrics. This number can be used to detect network partitions by observing the ratio of reachable routes to total routes. Routes with unreachable metrics, routes in a holddown state, and routes that have aged out are not considered reachable.

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; **MBR Operational Status** field added.

Related Commands

ip dvmrp admin-state	Globally enables or disables DVMRP protocol on the switch.
ip dvmrp flash-interval	Configures the minimum flash update interval value.
ip dvmrp graft-timeout	Configures the graft message retransmission value.
ip dvmrp neighbor-timeout	Configures the neighbor timeout.
ip dvmrp prune-lifetime	Indicates the length of time a prune will be in effect.
ip dvmrp prune-timeout	Configures the prune packet retransmission value.
ip dvmrp report-interval	Configures the route report interval.
ip dvmrp route-holddown	Configures the time during which DVMRP routes are kept in a hold down state.
ip dvmrp route-timeout	Configures the route expiration timeout value.
ip dvmrp subord-default	Configures the neighbor probe interval time.

MIB Objects

```
alaDvmrpConfigMIBGroup
   alaDvmrpAdminStatus
   alaDvmrpRouteReportInterval
   alaDvmrpFlashUpdateInterval
   alaDvmrpNeighborTimeout
   alaDvmrpRouteExpirationTimeout
   alaDvmrpRouteHoldDown
   alaDvmrpNeighborProbeInterval
   alaDvmrpPruneLifetime
   alaDvmrpPruneRetransmission
   alaDvmrpGraftRetransmission
   alaDvmrpInitNbrAsSubord
dvmrpGeneralGroup
   dvmrpNumRoutes
   dvmrpReachableRoutes
```

show ip dvmrp interface

Displays information for all multicast-capable interfaces *or* for a specified interface. This command also provides options to display only DVMRP-enabled or DVMRP-disabled interfaces.

show ip dvmrp interface [*ip_address* **|** *interface_name* **| enabled | disabled]**

Syntax Definitions

ip_address	Specifies a particular interface IP address.
interface_name	The name of the interface.
enabled	Displays a list of all interfaces (i.e., VLAN router ports) on which DVMRP is currently *enabled*.
disabled	Displays a list of all interfaces (i.e., VLAN router ports) on which DVMRP is currently *disabled*.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- If no optional syntax is specified in the command line, the entire interface table is displayed.
- For an interface to show as **enabled** in the **show ip dvmrp interface** or **show ip dvmrp interface enabled** output, the interface must be both administratively *and* operationally enabled. Although the interface does not have to be passing traffic, at least one VLAN router port must be operational on the corresponding DVMRP-enabled VLAN.
- To view the Generation ID being used on a particular interface, you must include the interface IP address in the command line.

Examples

```
-> show ip dvmrp interface

Total 4 Interfaces

Interface Name      Vlan  Metric  Admin-Status  Oper-Status  BFD-Status MBR-Default
------------------+-----+------+-------------+------------+----------+-----------
vlan-4                4       1   Disabled      Disabled      Disabled   Disabled
vlan-6                6       1    Enabled       Enabled      Disabled    Enabled
```

```
-> show ip dvmrp interface enabled

Total 1 Interfaces

Interface Name      Vlan  Metric  Admin-Status  Oper-Status  BFD-Status MBR-Default
------------------+-----+------+-------------+-------------+----------+-----------
vlan-6                 6       1   Enabled       Enabled       Disabled   Enabled
```

output definitions

Interface Name	The name of the interface.
Vlan	The associated VLAN ID.
Tunnel	Indicates whether there is a DVMRP tunnel currently configured on the interface.
Metric	The current metric value. A metric is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.
Admin-Status	The current administrative status of the corresponding interface. Options include **Enabled** or **Disabled**. An interface can be configured for DVMRP without being operational. To change the DVMRP Admin-status for an individual interface, refer to the **ip dvmrp interface** command.
Oper-Status	The current operational status of the corresponding multicast-capable interface. Options include **Enabled** or **Disabled**. For an interface to be DVMRP-operational, the global DVMRP status must be enabled and the individual interface must be DVMRP-enabled. To change the global DVMRP status, refer to the **ip dvmrp admin-state** command.
BFD-Status	Not supported in the current release.
MBR-Default	Whether or not the DVMRP interface will advertise a default route when the interface is configured on a Multicast Border Router. Options include **Enabled** or **Disabled**. Configured through the **ip dvmrp interface mbr-default-information** command.

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; **MBR-Default** field added.

Related Commands

ip dvmrp interface	Enables or disables the DVMRP protocol on a specified interface.

MIB Objects

```
dvmrpInterfaceGroup
   dvmrpInterfaceLocalAddress
   dvmrpInterfaceMetric
   dvmrpInterfaceStatus
alaDvmrpIfAugTable
   alaDvmrpIfMbrDefaultInfoStatus
```

show ip dvmrp neighbor

Displays the DVMRP neighbor table. The DVMRP neighbor table displays either all neighboring DVMRP routers, or a specified neighboring DVMRP router.

show ip dvmrp neighbor [*ip_address***]**

Syntax Definitions

ip_address	Specifies a particular IP address for a neighboring DVMRP router.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

If a neighbor IP address is not specified, the entire DVMRP Neighbor Table is displayed.

Examples

```
-> show ip dvmrp neighbor

Neighbor Address   Intf Name     Uptime      Expires     GenID     Vers  State
----------------+------------+-----------+-----------+----------+------+-------
143.209.92.214    vlan-2      00h:09m:12s 00h:00m:06s 546947509 3.255  active
```

output definitions

Neighbor Address	The 32-bit IP address of the DVMRP neighbor's router interface.
Itnf Name	The interface name of the neighbor's router.
Uptime	The amount of time the neighbor has been running, displayed in hours, minutes, and seconds.
Expires	The amount of time remaining before the neighbor expires, displayed in hours, minutes, and seconds.
GenID	The generation ID for the DVMRP neighbor. This value is used by neighboring routers to detect whether the DVMRP routing table should be resent.
Version	The DVMRP version number for the neighbor.
State	The current state of the DVMRP neighbor. Options include **active** and **down**.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp neighbor-interval	Configures the neighbor probe interval time.
ip dvmrp neighbor-timeout	Configures the neighbor timeout.

MIB Objects

```
dvmrpNeighborTable
   dvmrpNeighborAddress
   dvmrpNeighborIfIndex
   dvmrpNeighborUpTime
   dvmrpNeighborExpiryTime
   dvmrpNeighborGenerationId
   dvmrpNeighborMajorVersion
   dvmrpNeighborMinorVersion
   dvmrpNeighborState
```

show ip dvmrp nexthop

Displays DVMRP next hop entries. This command is used to show the list of next hops on outgoing interfaces to which IP multicast datagrams from particular sources are routed.

show ip dvmrp nexthop [*ip_address ip_mask***]**

Syntax Definitions

ip_address	Specifies a source IP address for which DVMRP next hop entries will be displayed.
ip_mask	Specifies a source IP mask for which DVMRP next hop entries will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

If an IP address and IP mask are not specified, the entire DVMRP Next Hop table is displayed.

Examples

```
-> show ip dvmrp nexthop 172.22.2.115 255.255.255.0

Src Address/Mask       Interface Name     Vlan    Hop Type
-------------------+-------------------+-------+----------

     172.22.2.115/24  vlan-2               2      branch
```

output definitions

Src Address/Mask	The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
Interface Name	The name of the interface.
Vlan	The associated VLAN ID.
Hop Type	The hop type of the associated entry. Options include **leaf** or **branch**. If the next hop VLAN has a DVMRP neighbor attached to it, the hop type will be displayed as **branch**.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
dvmrpRouteNextHopTable
   dvmrpRouteNextHopSource
   dvmrpRouteNextHopSourceMask
   dvmrpRouteNextHopIfIndex
   dvmrpRouteNextHopType
```

show ip dvmrp prune

Displays DVMRP prune entries that have been sent upstream.

show ip dvmrp prune [*group_address source_address source_mask***]**

Syntax Definitions

group_address	Specifies a pruned group address.
source_address	Specifies a source IP address.
source_mask	Specifies a source IP mask.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

If a group address, source address, and source mask are not specified, the entire Prune table is displayed.

Examples

```
-> show ip dvmrp prune

Group Address     Source Address/Mask    Expires
-----------------+---------------------+-------------
225.0.0.4           143.209.92.14/24    00h:00m:30s
```

output definitions

Group Address	The 32-bit multicast group address.
Source Address/Mask	The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
Expires	The amount of time remaining before the current prune state expires, displayed in hours, minutes, and seconds.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp prune-lifetime	Indicates the length of time a prune will be in effect.
ip dvmrp prune-timeout	Configures the prune packet retransmission value.

MIB Objects

```
dvmrpPruneTable
   dvmrpPruneGroup
   dvmrpPruneSource
   dvmrpPruneSourceMask
   dvmrpPruneExpiryTime
```

show ip dvmrp route

Displays the DVMRP routes that are being advertised to other routers.

show ip dvmrp route [*ip_address ip_mask***]**

Syntax Definitions

ip_address	The 32-bit source IP address representing route(s).
ip_mask	A 32-bit number that determines the subnet mask for the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

If a source IP address and IP mask are not specified, the entire DVMRP route table is displayed.

Examples

```
-> show ip dvmrp route
Legends:  Flags:  L = Local, R = Remote, F = Flash, H = Holddown, I = Invalid
     Address/Mask        Gateway       Metric     Age      Expires  Flags
------------------+-----------------+------+-----------+---------+-----
       11.0.0.0/8     55.0.0.5           2    00h:13m:14s  02m:07s    R
       22.0.0.0/8     44.0.0.4           2    00h:33m:14s  02m:15s    R
       44.0.0.0/8           -            1    05h:24m:59s     -       L
       55.0.0.0/8           -            1    05h:24m:59s     -       L
       66.0.0.0/8     44.0.0.4           2    00h:03m:11s  02m:15s    R
```

output definitions

Address/Mask	The 32-bit IP address for the router interface, along with the corresponding subnet mask. The interface's subnet mask is shown using the CIDR prefix length: 255.0.0.0 equals /8; 255.255.0.0 equals / 16; 255.255.255.0 equals /24, etc.
Gateway	The corresponding 32-bit gateway address. Because it is not applicable, no gateway address is displayed for local routes.
Metric	The current metric value. A metric is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.
Age	The current age of the DVMRP route, displayed in hours, minutes, and seconds.

output definitions (continued)

Expires	The expiration time for the corresponding route. Because it is not applicable, no expiration time is displayed for local routes.
Flags	The flag type of a particular DVMRP route. Options include **L** (Local), **R** (Remote), **F** (Flash), **H** (Holddown), and **I** (Invalid).

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp report-interval	Configures the route report interval.
ip dvmrp route-holddown	Configures the time during which DVMRP routes are kept in a hold down state.
ip dvmrp route-timeout	Configures the route expiration timeout value.

MIB Objects

```
dvmrpRouteTable
   dvmrpRouteSource
   dvmrpRouteSourceMask
   dvmrpRouteMetric
   dvmrpRouteExpiryTime
   dvmrpRouteUpTime
```

show ip dvmrp tunnel

Displays DVMRP tunnel entries.

show ip dvmrp tunnel [*local_address remote_address***]**

Syntax Definitions

local_address	The IP address of a particular local router interface. The local router interface IP address is an identifier for the local end of the DVMRP tunnel.
remote_mask	The IP address of a particular remote router interface. The remote router interface IP address is an identifier for the remote end of the DVMRP tunnel.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- If optional local and remote IP address information is not specified, entire DVMRP Tunnels table is displayed.
- The local IP address of the tunnel must match the IP address of an existing DVMRP-enabled IP interface.

Examples

```
-> show ip dvmrp tunnel

Interface Name       Local Address     Remote Address    TTL    Status
-------------------+-----------------+-----------------+-----+----------
vlan-2              143.209.92.203   12.0.0.1          255    Enabled
```

output definitions

Interface Name	The interface name.
Local Address	The 32-bit local IP address for the DVMRP tunnel.
Remote Address	The 32-bit remote IP address for the DVMRP tunnel.
TTL	The current Time to Live (TTL) value. A value of 0 indicates that the value is copied from the payload's header. Valid range from 0–255.
Status	The corresponding interface status. Options include **Enabled** or **Disabled**. If the interface specified by the local address has been configured and is operationally enabled, the status is **Enabled**. If the interface is down, the value displayed is **Disabled**.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip interface tunnel	Adds or deletes a DVMRP tunnel.
show ip dvmrp	Configures the TTL value for the tunnel defined for the specified local address and remote address.

MIB Objects

```
tunnelIfTable
   tunnelIfLocalAddress
   tunnelIfRemoteAddress
   tunnelIfHopLimit
dvmrpInterfaceGroup
   dvmrpInterfaceStatus
```

33 PIM Commands

Protocol-Independent Multicast (PIM) is an IP multicast routing protocol that uses routing information provided by unicast routing protocols, such as RIP and OSPF. Note that PIM is not dependent on any particular unicast routing protocol. Sparse mode PIM (PIM-SM) contrasts with flood-and-prune dense mode multicast protocols, such as DVMRP and PIM Dense Mode (PIM-DM), in that multicast forwarding in PIM-SM is initiated only through specific requests.

Downstream routers must explicitly join PIM-SM distribution trees to receive multicast streams on behalf of directly connected receivers or other downstream PIM-SM routers. This paradigm of receiver-initiated forwarding makes PIM ideal for network environments where receiver groups are thinly populated and bandwidth conservation is a concern, such as in wide area networks (WANs).

PIM-SIM builds unidirectional shared trees that are rooted at a Rendezvous Point (RP) multicast router. Bidirectional PIM (BIDIR-PIM) is a variant of PIM-SM that builds bidirectional shared trees also rooted at an RP. However, BIDIR-PIM forwards packets from the source to the RP without the overhead of encapsulation or source-specific states.

PIM-DM uses RPF (Reverse Path Forwarding) to prevent looping of multicast datagrams while flooding. If some areas of the network do not have group members, PIM-DM will prune the forwarding branch by instantiating the prune state.

PIM-DM differs from PIM-SM in two essential ways:

- There are no periodic joins transmitted, only explicitly triggered prunes and grafts.
- There is no Rendezvous Point (RP). This is particularly important in networks that cannot tolerate a single point of failure.

The OmniSwitch implementation of PIM can also be configured in an IPv6 environment.

MIB information for the PIM commands is as follows:

Filename: ALCATEL-IND1-VIRTUALROUTER-MIB.mib
Module: alcatelIND1VirtualRouterMIB

Filename: ALCATEL-IND1-PIM-MIB.mib
Module: alcatelIND1PIMMIB

Filename: PIM-BSR-MIB.mib
Module: pimBsrMIB

Filename: PIM-STD-MIB.mib
Module: pimStdMIB

A summary of the available commands is listed here:

ip load pim
ip pim sparse admin-state
ip pim bidir admin-state
ip pim dense admin-state
ip pim rp-hash admin-state
ip pim ssm group
ip pim dense group
ip pim cbsr
ip pim static-rp
ip pim anycast-rp
ip pim candidate-rp
ip pim rp-threshold
ip pim keepalive-period
ip pim max-rps
ip pim probe-time
ip pim register checksum
ip pim register-suppress-timeout
ip pim register-rate-limit
ip pim spt admin-state
ip pim state-refresh-interval
ip pim state-refresh-limit
ip pim state-refresh-ttl
ip pim interface
ip pim neighbor-loss-notification-period
ip pim invalid-register-notification-period
ip pim invalid-joinprune-notification-period
ip pim rp-mapping-notification-period
ip pim interface-election-notification-period
ip pim nonbidir-hello-notification-period
ip pim df-abort
ip pim mbr all-sources
ip pim df-periodic-interval
ip pim bfd-state
ip pim bfd-state all-interfaces
ip pim interface bfd-state
ip pim bidir ssm-compat
ip pim bidir fast-join
ip pim sparse asm-fast-join
ip pim sparse ssm-fast-join
ip pim joinprune-packing
show ip pim sparse
show ip pim dense
show ip pim ssm group
show ip pim dense group
show ip pim neighbor
show ip pim candidate-rp
show ip pim group-map
show ip pim interface
show ip pim static-rp
show ip pim anycast-rp
show ip pim cbsr
show ip pim bsr
show ip pim notifications
show ip pim groute
show ip pim sgroute
show ip pim df-election
ipv6 pim sparse admin-state
ipv6 pim bidir admin-state
ipv6 pim dense admin-state
ipv6 pim ssm group
ipv6 pim dense group
ipv6 pim cbsr
ipv6 pim static-rp
ipv6 pim anycast-rp
ipv6 pim candidate-rp
ipv6 pim rp-switchover
ipv6 pim register-rate-limit
ipv6 pim spt admin-state
ipv6 pim interface
ipv6 pim bfd-state
ipv6 pim bfd-state all-interfaces
ipv6 pim interface bfd-state
ipv6 pim bidir ssm-compat
ipv6 pim bidir fast-join
ipv6 pim sparse asm-fast-join
ipv6 pim sparse ssm-fast-join
ipv6 pim joinprune-packing
show ipv6 pim sparse
show ipv6 pim dense
show ipv6 pim ssm group
show ipv6 pim dense group
show ipv6 pim interface
show ipv6 pim neighbor
show ipv6 pim static-rp
show ipv6 pim anycast-rp
show ipv6 pim group-map
show ipv6 pim candidate-rp
show ipv6 pim cbsr
show ipv6 pim bsr
show ipv6 pim groute
show ipv6 pim sgroute
show ipv6 pim df-election

ip load pim

Dynamically loads PIM to memory.

ip load pim

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command must be executed before PIM can run on the switch.
- This command is supported in both IPv4 and IPv6 PIM.
- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

Examples

```
-> ip load pim
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim sparse admin-state	Globally enables or disables the PIM-SM protocol on the switch.
ip pim bidir admin-state	Globally enables or disables the BIDIR-PIM protocol on the switch.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
ip pim dense admin-state	Globally enables or disables PIM-DM protocol on the switch.
show ip pim dense	Displays the status of the various global parameters for the PIM Dense mode.
ipv6 pim sparse admin-state	Enables or disables IPv6 PIM-SM (sparse mode) globally for IPv6.
ipv6 pim bidir admin-state	Enables or disables IPv6 BIDIR-PIM (bidirectional) globally for IPv6.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.
ipv6 pim dense admin-state	Enables or disables the IPv6 PIM-DM (dense mode) globally for IPv6.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaVrConfigTable
   alaVrConfigPimStatus
```

ip pim sparse admin-state

Globally enables or disables PIM-SM protocol on the switch.

ip pim sparse admin-state {enable | disable}

Syntax Definitions

enable	Globally enables PIM-SM on the switch.
disable	Globally disables PIM-SM on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command must be set to **enable** before PIM-SM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 33-3 for more information.
- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

Examples

```
-> ip pim sparse admin-state enable
-> ip pim sparse admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminStatus
```

ip pim bidir admin-state

Globally enables or disables the BIDIR-PIM protocol on the switch.

ip pim bidir admin-state {enable | disable}

Syntax Definitions

enable	Globally enables BIDIR-PIM on the switch.
disable	Globally disables BIDIR-PIM on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command must be set to **enable** before BIDIR-PIM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 33-3 for more information.
- BIDIR-PIM is a variant of PIM-SM, which means that PIM-SM must also be globally enabled on the switch.

Examples

```
-> ip pim bidir admin-state enable
-> ip pim bidir admin-state disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmBidirStatus
```

ip pim dense admin-state

Globally enables or disables PIM-DM protocol on the switch.

ip pim dense admin-state {enable | disable}

Syntax Definitions

enable	Globally enables PIM-DM on the switch.
disable	Globally disables PIM-DM on the switch.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command must be set to **enable** before PIM-DM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 33-3 for more information.
- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

Examples

```
-> ip pim dense admin-state enable
-> ip pim dense admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmAdminStatus
```

ip pim rp-hash admin-state

Configures the version of the hashing algorithm that the Rendezvous Point (RP) hashing function will use to select an RP.

ip pim rp-hash admin-state {enable | disable}

Syntax Definitions

enable	Applies the newer version of the hashing algorithm.
disable	Applies the legacy version of the hashing algorithm.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The RP hashing function is applied when selecting an RP from two or more equal group-range-to-RP mappings.
- To maintain interoperability between PIM routers, make sure all routers have the same setting for the RP hash function. For example, this function is enabled for all PIM routers or this function is disabled for all PIM routers.

Examples

```
-> ip pim rp-hash admin-state enable
-> ip pin rp-hash admin-state disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmRPHashStatus
```

ip pim ssm group

Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).

ip pim ssm group *group_address/prefix_length* **[[no] override] [priority** *priority***]**

no ip pim ssm group *group_address/prefix_length*

Syntax Definitions

group_address	Specifies a 32-bit group address.
/prefix_length	Specifies the prefix length of the multicast group.
override	Specifies the static SSM mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
priority	Specifies the preference value to be used for this static SSM mode configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a SSM mode group mapping.
- The PIM Source-Specific Multicast (SSM) mode for the default SSM address range (232.0.0.0 through 232.255.255.255) reserved by the Internet Assigned Numbers Authority is not enabled automatically and needs to be configured manually to support SSM.
- You can also map additional multicast address ranges for the SSM group using this command. However, the multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the **override** option.
- Note that once the priority option has been defined, a value of 65535 can be used to unset the priority

Examples

```
-> ip pim ssm group 225.0.0.0/24 priority 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim ssm group	Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
pimStaticRPTable
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPPimMode
   pimStaticRPPrecedence
   pimStaticRPOverrideDynamic
   pimStaticRPRowStatus
```

ip pim dense group

Statically maps the specified IP multicast group(s) to the PIM Dense mode (DM).

ip pim dense group *group_address/prefix_length* **[[no] override] [priority** *priority***]**

no ip pim dense group *group_address/prefix_length*

Syntax Definitions

group_address	Specifies a 32-bit group address.
/prefix_length	Specifies the prefix length of the multicast group.
override	Specifies that this static Dense mode mapping configuration should override the dynamically learned group mapping information for the specified group(s).
priority	Specifies the preference value to be used for this static configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a dense mode group mapping.
- This command specifies the mode as Dense (PIM-DM) for the specified multicast group address.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to unset the priority.

Examples

```
-> ip pim dense group 225.0.0.0/24 priority 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ip pim dense group	Displays the static configuration of multicast group mappings for PIM-Dense Mode (DM).
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimdmDenseGroupTable
   alaPimdmDenseGroupGrpAddress
   alaPimdmDenseGroupGrpPrefixLength
   alaPimdmDenseGroupOverrideDynamic
   alaPimdmDenseGroupPrecedence
   alaPimdmDenseGroupRowStatus
```

ip pim cbsr

Configures the local router as the Candidate-BSR for the PIM domain.

ip pim cbsr *ip_address* **[priority** *priority***] [mask-length** *bits***]**

no ip pim cbsr *ip_address*

Syntax Definitions

ip_address	Specifies the 32-bit address that the local router uses to advertise itself as a Candidate-BSR.
priority	Specifies the priority value of the local router as a Candidate-BSR. The higher the value, the higher the priority. Values may range from 0–255.
bits	Specifies a 32-bit mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group).Values may range from 1–32.

Defaults

parameter	default
priority	64
bits	30

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the local routers candidature as the BSR.
- This command is supported only in the sparse mode.
- The information configured using this command is used in the Bootstrap messages.
- Candidate-BSRs also avoid a single point of failure in a PIM domain.

Examples

```
-> ip pim cbsr 50.1.1.1 priority 100 mask-length 4
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim cbsr	Displays the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBsrCandidateBSRTable
   pimBsrCandidateBSRAddress
   pimBsrCandidateBSRPriority
   pimBsrCandidateBSRHashMaskLength
   pimBsrCandidateBSRRowStatus
```

ip pim static-rp

Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

ip pim static-rp *group_address/prefix_length rp_address* **[[no] bidir] [[no] override] [priority** *priority***]**

no ip pim static-rp *group_address/prefix_length rp_address*

Syntax Definitions

group_address	Specifies a 32-bit group address.
/prefix_length	Specifies the prefix length of the multicast group.
rp_address	Specifies a 32-bit Rendezvous Point (RP) address.
bidir	Creates the static RP entry for use in the Bidirectional PIM (BIDIR-PIM) mode.
override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
priority	Specifies the preference value to be used for the static RP configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the **priority** option is not set, the **override** option is set to false, and the **bidir** option is set to false.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a static RP configuration.
- Specifying the priority value obsoletes the **override** option.
- If the **bidir** parameter option is not specified with this command, the static RP entry is created for use in the ASM mode.
- The PIM Source-Specific Multicast (SSM) mode for the default SSM address range (232.0.0.0 through 232.255.255.255) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM. You can also map additional multicast address ranges for the SSM group. However, the multicast groups in the reserved address range can be mapped only to the SSM mode.
- This command is supported only in the sparse mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Note that once the priority option has been defined, a value of 65535 can be used to unset the priority

- To view current static RP configuration settings, use the **show ip pim static-rp** command.

Examples

```
-> ip pim static-rp 225.0.0.0/24 10.1.1.1 priority 10
-> ip pin static-rp 225.0.0.0/24 10.1.1.1 bidir overide
-> no ip pin static-rp 225.0.0.0/24 10.1.1.1
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **bidir** parameter added.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim static-rp	Displays the PIM static RP table for ASM mode, which includes the group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the static RP configuration (i.e., enabled or disabled).
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
pimStaticRPTable
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPRPAddress
   pimStaticRPPimMode
   pimStaticRPOverrideDynamic
   pimStaticRPPrecedence
   pimStaticRPRowStatus
```

ip pim anycast-rp

Configures the anycast RP set, which is the set of all routers that would act as the RP.

ip pim anycast-rp *anycast_rp_address rp_address*

no ip pim anycast-rp *anycast_rp_address rp_address*

Syntax Definitions

anycast-rp-address	Specifies the anycast RP address.
rp_address	Specifies a 32-bit Rendezvous Point (RP) address of a router that is a member of the anycast RP set.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the no form of this command to delete an anycast RP configuration.
- The RP specified by anycast-RP-address is the RP in the anycast RP set. This address must be the same as the RP address in the Static-RP configuration used with the '**ip pim static-rp**' command if static RP configuration is being used.
- It is recommended not to use Loopback0 as the anycast RP address since Loopback0 is often used as the Router ID by default with the unicast routing protocols. Hence, it is recommended. to use one of the additional LoopbackX interfaces for the anycast RP address, but it is not mandatory to be a LoopbackX address.
- The RP specified by rp-address defines the IP address of the prospective RP. This address must be different than the anycast RP address and is used in communication between the different RPs in the anycast RP set. This configuration must be the same on all routers in the Anycast-RP set.
- There must be a separate entry for each of the RPs participating in anycast RP set, including an entry for the local router.This configuration defining the anycast RP set must be the same on all routers participating in anycast RP.
- It is recommended to configure PIM register rate limiting (see **ip pim register-rate-limit**) to limit the sending of PIM register messages with Anycast RP.
- Ensure SPT is enabled (see **ip pim spt admin-state**) when using Anycast RP. If SPT is globally disabled, and Anycast RP configuration is added, this configuration will be ignored for all groups that are operating in Anycast-RP mode.

Examples

```
-> ip pim static-rp 224.0.0.0/4 10.10.10.1
-> ip pim anycast-rp 10.10.10.1 10.1.1.1
```

```
-> ip pim anycast-rp 10.10.10.1 10.1.1.2

-> no ip pim anycast-rp 10.10.10.1 10.1.1.2
```

Release History

Release 8.6R2; command introduced.

Related Commands

ip pim static-rp	Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).
show ip pim anycast-rp	Displays the anycast RP table, which includes the anycast RP address, the RP address, if its the local router, and the current status of the anycast RP configuration

MIB Objects

```
pimAnycastRPSetTable
   pimAnycastRPSetAddressType
   pimAnycastRPSetAnycastAddress
   pimAnycastRPSetRouterAddress
   pimAnycastRPSetRowStatus
```

ip pim candidate-rp

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IP multicast group(s).

ip pim candidate-rp *rp_address group-address/prefix_length* **[[no] bidir] [priority** *priority***] [interval** *seconds***]**

no ip pim candidate-rp *rp_address group-address/prefix_length*

Syntax Definitions

rp_address	Specifies a 32-bit address that will be advertised as a Candidate-RP.
group_address	Specifies a 32-bit group address for which the local router will advertise itself as a Candidate-RP.
/prefix_length	Specifies the prefix length of the multicast group.
bidir	Creates a C-RP entry for use in the Bidirectional PIM (BIDIR-PIM) mode.
priority	Specifies the priority value of the Candidate-RP. Values may range from 0 to 192. The lower the value, the higher the priority.
seconds	Specifies the interval at which the C-RP advertisements are sent to the bootstrap router, in seconds. Values may range from 1 to 300.

Defaults

parameter	default
[no] bidir	**no bidir**
priority	192
seconds	60

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a C-RP for a particular multicast group.
- The specified *rp_address* must belong to a PIM enabled interface.
- Only one RP address is supported per switch. If multiple C-RP entries are defined, they must specify the same *rp-address.*
- If the **bidir** parameter option is not specified with this command, the C-RP entry is created for use in the ASM mode.
- The priority and the interval values are used by the switch. If they are modified for one entry, the switch will modify these for all the C-RP entries.

- This command is supported only in the sparse mode.

Examples

```
-> ip pim candidate-rp 50.1.1.1 225.0.0.0/24 priority 100 interval 100
-> ip pin candidate-rp 50.1.1.1 225.0.0.0/24 bidir priority 100 interval 100
-> no ip pim candidate-rp 50.1.1.1 225.0.0.0/24
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **bidir** parameter added.

Related Commands

show ip pim candidate-rp	Displays the IP multicast groups for which the local router will advertise itself as a Candidate-RP.

MIB Objects

```
pimBsrCandidateRPTable
   pimBsrCandidateRPAddress
   pimBsrCandidateRPGroupAddress
   pimBsrCandidateRPGroupPrefixLength
   pimBsrCandidateRPBidir
   pimBsrCandidateRPPriority
   pimBsrCandidateRPAdvInterval
   pimBsrCandidateRPRowStatus
```

ip pim rp-threshold

Specifies the data rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing a source-specific (S, G) Join message toward the source.

ip pim rp-threshold *bps*

Syntax Definitions

bps	The data rate value, in bits per second, at which the RP will attempt to switch to native forwarding (0–2147483647).

Defaults

parameter	default
bps	1

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is supported only in the sparse mode.
- To disable the RP threshold feature, specify a bits per second value of 0. When the RP threshold is disabled, the RP will never initiate an (S, G) Join message toward the source; the packets will be register-encapsulated to the RP. It will issue a (S, G) Join message upon receiving the first data packet, if its bits per second value is 1.
- To view the current RP threshold, use the **show ip pim sparse** command.

Examples

```
-> ip pim rp-threshold 131072
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the global parameters for PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmRPThreshold
```

ip pim keepalive-period

Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.

ip pim keepalive-period *seconds*

Syntax Definitions

seconds	Specifies the timeout value, in seconds (0-65535).

Defaults

parameter	default
seconds	210

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This timer is called the Keepalive Period in the PIM-SM specification and the Source Lifetime in the PIM-DM specification.
- This command includes support for both IPv4 PIM and IPv6 PIM.

Examples

```
-> ip pim keepalive-period 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
pim
   pimKeepalivePeriod
```

ip pim max-rps

Configures the maximum number of C-RP routers allowed in the PIM-SM domain.

ip pim max-rps *number*

Syntax Definitions

number	The maximum number of C-RP routers allowed in the PIM-SM domain (1–100).

Defaults

parameter	default
number	32

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is supported only in the sparse mode.
- This command is used with both IPv4 and IPv6 PIM-SM. The PIM-SM must be disabled before changing **max-rps** value.
- PIM-SM must be globally disabled before changing the maximum number of C-RP routers. To globally disable PIM-SM, refer to the **ip pim sparse admin-state** command on page 33-5.

Examples

```
-> ip pim max-rps 32
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim sparse admin-state	Globally enables or disables the PIM-SM protocol on the switch.
ipv6 pim sparse admin-state	Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmMaxRPs
```

ip pim probe-time

Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.

ip pim probe-time *seconds*

Syntax Definitions

seconds	The probe time, in seconds (1–300).

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used with both IPv4 and IPv6 PIM-SM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim probe-time 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmProbeTime
```

ip pim register checksum

Configures the application of the checksum function on sent and received register messages in the domain.

ip pim register checksum {header | full}

Syntax Definitions

header	Specifies that the checksum for registers is done only on the PIM header.
full	Specifies that the checksum is done over the entire PIM register message.

Defaults

parameter	default
header | full	**header**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The **full** option may be required for compatibility with older implementations of PIM-SM v2.
- This parameter setting must be consistent across the PIM domain.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim register checksum header
-> ip pim register checksum full
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmOldRegisterMessageSupport
```

ip pim register-suppress-timeout

Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.

ip pim register-suppress-timeout *seconds*

Syntax Definitions

seconds	The timeout value, in seconds (0–65535).

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is supported in both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim register-suppress-timeout 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
pim
   pimRegisterSuppressionTime
```

ip pim register-rate-limit

Configures the maximum number of PIM Register Packets that the Designated Router (DR) will send per second for each (S,G) entry.

ip pim register-rate-limit *pps*

Syntax Definitions

pps	The per (S,G) register rate limit in packets per second (0–65535).

Defaults

By default, the register rate limit is set to zero (no rate-limiting is applied to outgoing PIM Register messages).

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Setting the register rate limit to zero (the default) disables register rate limiting.
- Rate limiting is applied on a per (S,G) flow basis.
- This command is supported in both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim register-rate-limit 100
-> ip pim register-rate-limit 0
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfigTable
   alaPimsmRegisterRateLimit
```

ip pim spt admin-state

Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first data packet is received.

ip pim spt admin-state {enable | disable}

Syntax Definitions

enable	Enables last hop DR switching to the SPT.
disable	Disables last hop DR switching to the SPT.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is supported only in the sparse mode.
- As mentioned above, if SPT status is enabled, last hop DR switching to the SPT begins once the first data packet is received.
- To view whether SPT status is currently enabled (default) or disabled, use the **show ip pim sparse** command.

Examples

```
-> ip pim spt admin-state enable
-> ip pim spt admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAdminSPTConfig
```

ip pim state-refresh-interval

Sets the interval between successive State Refresh messages originated by a router.

ip pim state-refresh-interval *seconds*

Syntax Definitions

seconds	The interval between successive State Refresh messages, in seconds. Values may range from 0 to 65535.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 PIM-DM and IPv6 PIM-DM.

Examples

```
-> ip pim state-refresh-interval 80
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ipv6 pim interface	Enables IPv6 PIM and configures the statistics.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
pim
   pimRefreshInterval
```

ip pim state-refresh-limit

Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.

ip pim state-refresh- limit *ticks*

Syntax Definitions

ticks	The limit at which the received State Refresh messages will not be forwarded, if the messages are received at less than the interval. Values may range from 0 to 65535.

Defaults

parameter	default
ticks	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 and IPv6.

Examples

```
-> ip pim state-refresh-limit 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ipv6 pim interface	Enables IPv6 PIM and configures the statistics.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmStateRefreshLimitInterval
```

ip pim state-refresh-ttl

Sets the Time to Live to be used in a router's originated State Refresh messages if the data packet's Time to Live is not recorded.

ip pim state-refresh- ttl *num*

Syntax Definitions

num	The Time to Live to be used. Values may range from 0 to 255.

Defaults

parameter	default
num	16

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 and IPv6 PIM-DM.

Examples

```
-> ip pim state-refresh-ttl 122
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ipv6 pim interface	Enables IPv6 PIM and configures the statistics.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmStateRefreshTimeToLive
```

ip pim interface

Enables PIM and configures PIM-related statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the interface.

ip pim interface *if_name*
[hello-interval *seconds***]**
[triggered-hello *seconds***]**
[joinprune-interval *seconds***]**
[hello-holdtime *seconds***]**
[joinprune-holdtime *seconds***]**
[prune-delay *milliseconds***]**
[override-interval *milliseconds***]**
[dr-priority *priority***]**
[prune-limit-interval *seconds***]**
[graft-retry-interval *seconds***]**
[df-election-robustness *messages***]**
[[no] stub]
[joinprune-mtu *bytes***]**
[joinprune-delay *milliseconds***]**

no ip pim interface *if_name*

Syntax Definitions

if_name	The interface name on which PIM is being enabled or disabled.
hello-interval *seconds*	The frequency at which PIM Hello messages are transmitted on a specified interface, in seconds. Values range from 0 to 18000.
triggered-hello *seconds*	Specifies the maximum time, in seconds, before a triggered PIM Hello message is sent on this interface. Values range from 0 to 60.
joinprune-interval *seconds*	The frequency at which periodic Join/Prune messages are sent on this interface, in seconds. Values range from 0 to 18000.
hello-holdtime *seconds*	Specifies the value set in the Holdtime field of PIM Hello messages sent on this interface, in seconds. Values range from 0 to 65535.
joinprune-holdtime *seconds*	Specifies the value inserted into the Holdtime field of the Join/Prune messages sent on this interface, in seconds.Values range from 0 to 65535.
prune-delay *milliseconds*	Specifies the value of the expected propagation delay between PIM routers on this network, inserted into the LAN prune-delay option of the Hello messages sent on this interface, in milliseconds. Values range from 0 to 32767.
override-interval *milliseconds*	Specifies the value inserted into the Override Interval field of the LAN prune-delay option of the Hello messages sent on this interface, in *milliseconds.* Values range from 0 to 65535.

dr-priority *priority*	Specifies the Designated Router priority inserted into the DR priority option on a specified interface. The DR priority option value can range between 1 to 192. A higher numeric value denotes a higher priority.
prune-limit-interval *seconds*	Specifies the minimum interval that must elapse between two successive prune messages sent on this interface, in seconds. Values range from 0 to 65535.
graft-retry-interval *seconds*	Specifies the minimum interval that must elapse between two successive graft messages sent on this interface, in seconds. Values range from 0 to 65535.
df-election-robustness *messages*	The minimum number of DF-Election messages that must be lost in order for the DF Election to fail on the specified interface. Values range from 1–65535. This value is used only by BIDIR-PIM
stub	Specifies the interface not to send any PIM packets through this interface, and to ignore received PIM packets.
joinprune-mtu *bytes*	Specifies the maximum size used for PIM Join/Prune packets sent out of the interface. Values range from 0 to 9198. *Supported only on the OmniSwitch 6860 and OmniSwitch 6900.*
joinprune-delay *milliseconds*	Specifies the Join/Prune delay interval in milliseconds. Values range from 0 to 32767. *Supported only on the OmniSwitch 6860 and OmniSwitch 6900.*

Defaults

parameter	default
hello-interval *seconds*	30
triggered-hello *seconds*	5
joinprune-interval *seconds*	60
hello-holdtime *seconds*	105
joinprune-holdtime *seconds*	210
prune-delay *milliseconds*	500
override-interval *milliseconds*	2500
dr-priority *priority*	1
prune-limit-interval *seconds*	60
graft-retry-interval *seconds*	3
df-election-robustness *messages*	3
stub	Disabled
joinprune-mtu *bytes*	0
joinprune-delay *milliseconds*	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a PIM interface.
- PIM must be enabled globally on the switch before it runs on the interface. To globally enable or disable PIM-SM on the switch, refer to the **ip pim sparse admin-state** command on page 33-5. To enable or disable PIM-DM on the switch, refer to the **ip pim dense admin-state** command on page 33-7.
- Specifying zero for the hello-interval represents an infinite time, in which case periodic PIM Hello messages are not sent.
- Specifying zero for the joinprune-interval represents an infinite time, in which case periodic PIM Join/Prune messages are not sent.
- Specifying the value of 65535 for hello-holdtime represents an infinite time. If a PIM router gets Hello packet from a neighbor with its hello-holdtime value as infinite time, then the PIM router will not time out the sender(neighbor). It is recommended that you should use a hello-holdtime interval that is 3.5 times the value of the hello-interval, or 65535 seconds if the hello-interval is set to zero.
- Specifying the value of 65535 for joinprune-holdtime represents an infinite time. The receipt of Join/Prune messages with its joinprune-holdtime value as infinite time, then this specifies an infinite holdtime for the particular join/prune message. It is recommended that you use a joinprune-holdtime interval that is 3.5 times the value of the Join/Prune interval defined for the interface, or 65535 seconds if the joinprune-interval is set to zero.
- The interface configured as a **stub** will not send any PIM packets through that interface, and any received PIM packets are also ignored. By default, a PIM interface is not set to be a stub one.
- The **graft-retry-interval** and **prune-limit-interval** options can be used only with the PIM-DM mode.
- If the IP interface on which PIM is enabled is bound to an SPB service, then PIM can operate over an SPB L3 VPN in-line routing configuration (supported only on the OmniSwitch 9900).
- By default, **joinprune-mtu** value is ‘0’ and the configured interface MTU value will be used in determining the maximum packet size that can be used in sending the packed messages. However, if the Join/Prune MTU configuration is specified, the actual maximum size used for PIM Join/Prune messages will be the smaller of the IP MTU value of the interface and the configured interface Join/Prune MTU value.
- The **joinprune-delay** interval is used to delay the sending of triggered Join/Prune messages and may be desirable to allow the packing of triggered Join.Prune messages due to bursts of protocol messages, which may result in subsequent bursts of triggered Join/Prune packets. The default value of ‘0’ implies no deferred processing and will result in no packing of triggered Join/Prune packets.

Examples

```
-> ip pim interface vlan-2 hello-interval 100 triggered-hello 10 joinprune-interval
100 hello-holdtime 350 joinprune-holdtime 400
-> no ip pim interface vlan-2
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **df-election-robustness** parameter added.
Release 8.6R1; **joinprune-mtu**, **joinprune-delay** parameters added.

Related Commands

show ip pim interface	Displays detailed PIM settings for a specific interface. In general, it displays PIM settings for all the interfaces if no argument is specified.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceStatus
   pimInterfaceHelloInterval
   pimInterfaceTrigHelloInterval
   pimInterfaceJoinPruneInterval
   pimInterfaceHelloHoldtime
   pimInterfaceJoinPruneHoldtime
   pimInterfaceDFElectionRobustness
   pimInterfacePropagationDelay
   pimInterfaceOverrideInterval
   pimInerfaceDRPriority
   pimInterfaceStubInterface
   pimInterfacePruneLimitInterval
   pimInterfaceGraftRetryInterval
alaPimInterfaceAugTable
   alaPimInterfaceJoinPruneMtu
   alaPimInterfaceJoinPruneDelay
```

ip pim neighbor-loss-notification-period

Specifies the minimum time that must elapse between PIM neighbor loss notifications originated by the router.

ip pim neighbor-loss-notification-period *seconds*

Syntax Definitions

seconds	Specifies the time value that must elapse between neighbor loss notifications, in seconds (0–65535).

Defaults

parameter	default
seconds	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The maximum value of 65535 represents an infinite time. The PIM neighbor loss notifications are never sent in case of infinite time.
- This command is used with both IPv4 and IPv6 PIM.

Examples

```
-> ip pim neighbor-loss-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
pim
   pimNeighborLossNotificationPeriod
```

ip pim invalid-register-notification-period

Specifies the minimum time that must elapse between the PIM invalid register notifications originated by the router.

ip pim invalid-register-notification-period *seconds*

Syntax Definitions

seconds	Specifies the minimum time value that must elapse between invalid register notifications, in seconds (10–65535).

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The default value of 65535 represents an infinite time. The PIM invalid register notifications are never sent in case of infinite time.
- The non-zero minimum allowed value provides resilience against the propagation of denial-of-service attacks from the data and control planes to the network management plane.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim invalid-register-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
pim
   pimInvalidRegisterNotificationPeriod
```

ip pim invalid-joinprune-notification-period

Specifies the minimum time that must elapse between the PIM invalid joinprune notifications originated by the router.

ip pim invalid-joinprune-notification-period *seconds*

Syntax Definitions

seconds	Specifies the minimum time value that must elapse between invalid joinprune notifications, in seconds (10–65535).

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The default value of 65535 represents an infinite time. The PIM invalid joinprune notifications are never sent in case of infinite time.
- The non-zero minimum allowed value provides resilience against the propagation of denial-of-service attacks from the control plane to the network management plane.
- This value is used with both IPv4 and IPv6 PIM.

Examples

```
-> ip pim invalid-joinprune-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
pim
   pimInvalidJoinPruneNotificationPeriod
```

ip pim rp-mapping-notification-period

Specifies the minimum time that must elapse between the PIM RP mapping notifications originated by the router.

ip pim rp-mapping-notification-period *seconds*

Syntax Definitions

seconds	Specifies the minimum time value that must elapse between RP mapping notifications, in seconds (0–65535).

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The default value of 65535 represents an infinite time. The RP mapping notifications are never sent in case of infinite time.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim rp-mapping-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
pim
   pimRPMappingNotificationPeriod
```

ip pim interface-election-notification-period

Specifies the minimum time that must elapse between the PIM interface election notifications originated by the router.

ip pim interface-election-notification-period *seconds*

Syntax Definitions

seconds	Specifies the minimum time value that must elapse between interface election notifications, in seconds (0–65535).

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The default value of 65535 represents an infinite time. The interface election notifications are never sent in case of infinite time.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim interface-election-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
pim
   pimInterfaceElectionNotificationPeriod
```

ip pim nonbidir-hello-notification-period

Specifies the minimum time that must elapse between notifications that a Bidirectional PIM (BIDIR-PIM) router transmits whenever the router receives a PIM Hello message that *does not* contain the Bidirectional Capable option.

ip pim nonbidir-hello-notification-period *seconds*

Syntax Definitions

seconds	The minimum time value that must elapse between notifications, in seconds. The valid range is 10–65535.

Defaults

parameter	default
seconds	65535

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The default value of 65535 represents an infinite time. This type of notification is never sent when this value is set to infinite time.
- The default minimum time is set to a non-zero value to provide resilience against the propagation of denial-of-service (DoS) attacks from the control plane to the network management plane.
- The Bidirectional Capable option indicates that a router is capable of participating as a BIDIR-PIM neighbor.
- This value is used with both IPv4 and IPv6 PIM.
- This command is only applicable if BIDIR-PIM is globally enabled for the switch.

Examples

```
-> ip pim nonbidir-hello-notification-period 1000
-> ip pin nonbidir-hello-notification-period 65535
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip pim df-abort	Configures whether or not the Designated Forwarder (DF) election process is aborted when a PIM Hello message received from a PIM neighbor does not contain the Bidirectional Capable option.
show ip pim notifications	Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmNonBidirHelloPeriod
```

ip pim df-abort

Configures whether or not the Designated Forwarder (DF) election process is stopped when a PIM Hello message received from a PIM neighbor does not contain the Bidirectional Capable option.

ip pim df-abort {enable | disable}

Syntax Definitions

enable	Administratively enables the DF abort operation (DF election is stopped).
disable	Administratively disables the DF abort operation (DF election is not stopped).

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The DF election process occurs between PIM routers that support BIDIR-PIM. When the DF abort option is disabled, this election process continues between the BIDIR-PIM routers.
- This command is only applicable if BIDIR-PIM is globally enabled for the switch.

Examples

```
-> ip pim df-abort enable
-> ip pin df-abort disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ip pim nonbidir-hello-notification-period	Specifies the minimum time between notifications that a BIDIR-PIM router transmits when the router receives a Hello message from a neighbor that does not contain the Bidirectional Capable option.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmBidirDFAbort
```

ip pim mbr all-sources

Configures whether or not PIM notifies DVMRP about the routes to all multicast sources learned. This command applies only when the local switch is operating as a Multicast Border Router (MBR).

ip pim mbr all-sources

no ip pim mbr all-sources

Syntax Definitions

N/A

Defaults

By default, PIM only notifies DVMRP about the routes for subnets directly connected to PIM interfaces.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable notification of all route sources learned.
- This command applies to both PIM-SM and PIM-DM. Note that PIM-SSM does not support MBR functionality.
- DVMRP advertises the routes received from PIM within the DVMRP domain using standard DVMRP mechanisms.

Examples

```
-> ip pim mbr all-sources
-> no ip pim mbr all-sources
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
ip mroute mbr	Configures the switch to operate as a Multicast Border Router to provide interoperability between PIM and DVMRP.
ip dvmrp interface mbr-default-information	Configures whether or not the DVMRP interface on a Multicast Border Router advertises a default route.

MIB Objects

```
alaPimGlobalConfig
   alaPimMbrAllSourcesStatus
```

ip pim df-periodic-interval

Sets the interval at which the Designated Forwarder (DF) for each Rendezvous Point Address (RPA) periodically announces its status in a Winner message.

ip pim df-periodic-interval *seconds*

Syntax Definitions

seconds	The time interval between successive Winner messages, in seconds. The valid range is 0–2000.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the value for this interval is set to zero, no messages are sent.
- This value is used with both IPv4 BIRDIR-PIM and IPv6 BIRDIR-PIM.
- Setting this interval value provides an additional degree of safety to ensure that two routers do not both consider themselves to be the DF for the same link.
- The periodic Winner messages will only occur for RPAs that have active groups, thus avoiding the periodic control traffic in areas of the network without senders or receivers for a particular RPA.

Examples

```
-> ip pim df-periodic-interval 80
-> ip pin df-periodic-interval 0
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmBidirPeriodicInterval
```

ip pim bfd-state

Enables or disables the registration of PIM with the BFD protocol.

ip pim bfd-state {enable | disable}

Syntax Definitions

enable	Enables BFD for PIM.
disable	Disables BFD for PIM.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- BFD must be globally enabled for the switch and PIM must be registered with BFD at the protocol level before PIM can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and PIM acts based upon the BFD message.
- Whenever a neighbor goes down, PIM will inform BFD to remove that neighbor from the BFD active list.

Examples

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of PIM with the BFD protocol:

```
-> ip pim bfd-state enable
-> ip pim bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd admin-state	Enables or disables the global BFD protocol status for the switch.
ip pim bfd-state all-interfaces	Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.
ip pim interface bfd-state	Enables or disables BFD monitoring on a specific PIM interface.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.

MIB Objects

```
alaPimGlobal
   alaPimBfdStatus
```

ip pim bfd-state all-interfaces

Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.

ip pim bfd-state all-interfaces {enable | disable}

Syntax Definitions

enable	Enables BFD for all the PIM interfaces.
disable	Disables BFD for all the PIM interfaces.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for PIM must be enabled before PIM can interact with BFD.

Examples

```
-> ip pim bfd-state all-interfaces enable
-> ip pim bfd-state all-interfaces disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim bfd-state	Enables or disables the registration of PIM with the BFD protocol.
ip pim interface bfd-state	Enables or disables BFD monitoring on a specific PIM interface.
show ip pim interface	Displays detailed PIM settings for a specific interface.

MIB Objects

```
alaPimGlobalConfig
   alaPimBfdAllInterfaceStatus
```

ip pim interface bfd-state

Enables or disables BFD monitoring for a specific PIM interface.

ip pim interface *if_name* **bfd-state {enable | disable}**

Syntax Definitions

if_name	The name of an existing PIM interface.
enable	Enables BFD for the specified PIM interface.
disable	Disables BFD for the specified PIM interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Registering PIM with BFD is required at the protocol level before PIM can interact with BFD.
- When BFD is enabled on the specified PIM interface, BFD monitors the connectivity to all neighbors known through the specified interface.

Examples

```
-> ip pim interface pimInt1 bfd-state enable
-> ip pim interface pimInt1 bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim bfd-state	Enables or disables the registration of PIM with the BFD protocol.
ip pim bfd-state all-interfaces	Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.
show ip pim interface	Displays detailed PIM settings for a specific interface.

MIB Objects

```
alaPimInterfaceAugTable
   alaPimBfdStatus
```

ip pim bidir ssm-compat

Configures the status of the Source-specific Multicast (SSM) compatibility mode. When enabled, a BIDIR-PIM router will support receiving IGMPv3 SSM joins and process them as a (*,G) join.

ip pim bidir ssm-compat {enable | disable}

Syntax Definitions

enable	Administratively enables BIDIR/SSM compatibility mode.
disable	Administratively disables BIDIR/SSM compatibility mode.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the SSM compatibility mode is disabled, SSM joins are ignored by the BIDIR-PIM router.
- This command is only applicable if BIDIR-PIM is globally enabled for the switch.

Examples

```
-> ip pim bidir ssm-compat enable
-> ip pim bidir ssm-compat disable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmBidirSsmCompat
```

ip pim bidir fast-join

Configures whether or not a BIDIR-PIM router will automatically create (*,G) routes in the hardware as soon as BIDIR (*,G) routes are learned.

ip pim bidir fast-join {enable | disable}

Syntax Definitions

enable	Administratively enables the BIDIR-PIM fast join functionality.
disable	Administratively disables the BIDIR-PIM fast join functionality.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is only applicable if BIDIR-PIM is globally enabled for the switch.
- When the BIDIR fast join functionality is enabled, convergence of multicast traffic may occur faster because the (*,G) routes are already created before the actual multicast traffic is received.
- When the BIDIR fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.

Examples

```
-> ip pim bidir fast-join enable
-> ip pim bidir fast-join disable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmBidirFastJoin
```

ip pim sparse asm-fast-join

Configures whether or not a PIM Sparse router will automatically create (*,G) routes in the hardware as soon as the (*,G) routes are learned.

ip pim sparse asm-fast-join {enable | disable}

Syntax Definitions

enable	Administratively enables the PIM Sparse ASM fast join functionality.
disable	Administratively disables the PIM Sparse ASM fast join functionality.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is only supported in the PIM Sparse mode.
- When the PIM Sparse fast join functionality is enabled, convergence of multicast traffic may occur faster because the (*,G) routes are already created before the actual multicast traffic is received.
- When the PIM Sparse fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.
- This option should be used with caution due to the complicated nature of PIM ASM, which involves forwarding on the shared tree, the sending and receiving of PIM register packets, and switching to the SPT. As a result, only enable the ASM fast join function when there are no other locally attached sources, the router is not the RP, and the SPT is disabled.

Examples

```
-> ip pim sparse asm-fast-join enable
-> ip pim sparse asm-fast-join disable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmAsmFastJoin
```

ip pim sparse ssm-fast-join

Configures whether or not a PIM Sparse router will automatically create both PIM Sparse and SSM (S,G) routes in the hardware as soon as the (S,G) routes are learned.

ip pim sparse ssm-fast-join {enable | disable}

Syntax Definitions

enable	Administratively enables the PIM Sparse SSM fast join functionality.
disable	Administratively disables the PIM Sparse SSM fast join functionality.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is only supported in the PIM Sparse mode.
- When the PIM Sparse fast join functionality is enabled, convergence of multicast traffic may occur faster because the (S,G) routes are already created before the actual multicast traffic is received.
- When the PIM Sparse fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.

Examples

```
-> ip pim sparse ssm-fast-join enable
-> ip pim sparse ssm-fast-join disable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmSsmFastJoin
```

ip pim joinprune-packing

Enable or disable PIM Join/Prune message packing.

ip pim joinprune-packing {enable | disable}

Syntax Definitions

enable	Enable the PIM Join/Prune message packing.
disable	Disable the PIM Join/Prune message packing

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6860, 6900

Usage Guidelines

When this feature is disabled, Join/Prune messages are not packed.

Examples

```
-> ip pim joinprune-packing enable
-> ip pim joinprune-packing disable
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimGlobalConfig
   alaPimJoinPruneMsgPackingStatus
```

show ip pim sparse

Displays the status of the various global parameters for the PIM sparse mode.

show ip pim sparse

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip pim sparse
Status                     = disabled,
Keepalive Period           = 210,
Max RPs                    = 32,
Probe Time                 = 5,
Register Checksum          = header,
Register Suppress Timeout  = 60,
RP Threshold               = 1,
SPT Status                 = enabled,
BIDIR Status               = disabled,
BIDIR Periodic Interval    = 60,
BIDIR DF Abort Status      = disabled,
BFD Status                 = disabled,
MoFRR Status               = disabled,
MoFRR All Routes Status    = disabled,
MBR All Sources Status     = disabled,
MBR Operational Status     = disabled,
RP Hash Algorithm          = disabled,
ASM Fast Join              = disabled,
SSM Fast Join              = disabled,
BIDIR Fast Join            = disabled,
BIDIR SSM Compatibility    = enabled,
Register Rate Limit        = 100,
Join/Prune Message Packing = enable
```

output definitions

Status	The current global (i.e., switch-wide) status of PIM-SM. Options include **enabled** and **disabled**.
Keepalive Period	The duration of the Keepalive timer. The default value is 210.

output definitions (continued)

Max RPs	The maximum number of Rendezvous Points (RPs) allowed in the PIM-SM domain (1–100). The default value is 32.
Probe Time	The amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP. Values may range from 1 to 300. The default value is 5.
Register Checksum	The current application of the checksum function on register messages in the domain. Options include **header** and **full**. The default setting is **header**.
Register Suppress Timeout	The amount of time, in seconds, the Designated Router (DR) will stop sending registers to the Rendezvous Point (RP) once a Register-Stop is received (1–300). The default value is 60.
RP Threshold	Displays the current RP data rate threshold. This value indicates the rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing an (S, G) Join message toward the source. Values may range from 0 to 2147483647. The default value is 1. A value of 0 indicates that the feature is currently disabled.
SPT Status	The current status of last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). Options include **enabled** (the default) and **disabled**.
BIDIR Status	The current global status of Bidirectional PIM (BIDIR-PIM) for the switch. Options include **enabled** and **disabled** (the default).
BIDIR Periodic Interval	The amount of time, in seconds, between Winner messages the Designated Forwarder (DF) sends out to announce its status. The valid range is 0–2000. The default is 60 seconds.
BIDIR DF Abort Status	Indicates whether or not the DF election process is stopped when a BIDIR-PIM router receives a Hello message that does not contain the Bidirectional Capable option. When **enabled** DF election is stopped; when **disabled** (the default) DF election continues.
BFD Status	Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is **enabled** or **disabled** (the default) for the PIM router.
MoFRR Status **MoFRR All Routes Status**	Not supported in the current release.
MBR All Sources Status	Indicates whether or not PIM notifies DVMRP about the routes to all multicast sources learned. Options include **enabled** (routes to all sources) or **disabled** (only routes on PIM interfaces). This status only applies when the switch is operating in the Multicast Border Router (MBR) mode.
MBR Operational Status	Indicates whether or not PIM interaction with DVMRP is **enabled** or **disabled** on a MBR switch. MBR functionality is not operationally active until both PIM and DVMRP have at least one enabled and active interface.

output definitions (continued)

RP Hash Algorithm	The status of the RP hashing algorithm. When **enabled**, a newer version of the algorithm is in use; when **disabled** (the default), a legacy version of the algorithm is in use.
ASM Fast Join	*PIM Sparse fast join is not supported.*
SSM Fast Join	*PIM Sparse fast join is not supported.*
BIDIR Fast Join	*BIDIR-PIM fast join is not supported.*
BIDIR SSM Compatibility	The status of the SSM compatibility mode. When **enabled**, a BIDIR-PIM router will accept and process SSM joins as (*,G) joins; when **disabled** (the default), SSM joins are ignored.
Register Rate Limit	The per (S,G) register rate limit in packets per second.
Join/Prune Message Packing	The current status of PIM Join/Prune message packing. Options include **enabled** and **disabled**.

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; **MBR All Sources Status** and **MBR Operational Status** fields added.
Release 7.3.4; BIDIR fields added, **RP Hash Algorithm** field added.
Release 8.2.1.R02: **ASM Fast Join**, **SSM Fast Join**, **BIDIR Fast Join**, and **BIDIR SSM Compatibility** fields added.
Release 8.4.1.R02; **Register Rate Limit** field added.
Release 8.6R1; **Join/Prune Message Packing** field added.

Related Commands

ip pim sparse admin-state	Globally enables or disables PIM-SM protocol on the switch.
ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip pim keepalive-period	Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
ip pim max-rps	Configures the maximum number of C-RP routers allowed in the PIM-SM domain.
ip pim probe-time	Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.
ip pim register checksum	Configures the application of the checksum function on sent and received register messages in the domain.
ip pim register-suppress-timeout	Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.
ip pim register-rate-limit	Specifies the maximum number of PIM Register Packets that the Designated Router (DR) will send per second for each (S,G) entry.

ip pim rp-threshold	Specifies the data rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing a source-specific (S, G) Join message toward the source.
ip pim spt admin-state	Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first data packet is received.
ip pim bidir admin-state	Globally enables or disables BIDIR-PIM protocol on the switch.
ip pim df-periodic-interval	Configures the time interval at which the DF for each RP address periodically announces its status in a Winner message
ip pim df-abort	Configures whether or not the DF election process is stopped when a PIM Hello message received from a PIM neighbor does not contain the Bidirectional Capable option.
ip pim bfd-state	Enables or disables the registration of PIM with the BFD protocol.
ip pim mbr all-sources	Configures PIM to notify DVMRP of all learned routes to sources. This command only applies when the switch is operating in the Multicast Border Router mode.
ip pim rp-hash admin-state	Globally enables or disables the RP hashing algorithm version for the switch.
ip pim bidir ssm-compat	Configures the SSM compatibility mode for a BIDIR-PIM router.
ip pim joinprune-packing	Enable or disable PIM Join/Prune message packing.

MIB Objects

```
ALCATEL-IND1-PIM-MIB
alaPimsmGlobalConfig
   alaPimsmAdminStatus
   alaPimsmMaxRPS
   alaPimsmProbeTime
   alaPimsmOldRegisterMessageSupport
   alaPimsmRPThreshold
   alaPimsmAdminSPTConfig
   alaPimsmBidirStatus
   alaPimsmBidirPeriodicInterval
   alaPimsmBidirDFAbort
   alaPimMbrAllSourcesStatus
   alaPimMbrOperStatus
   alaPimsmRPHashStatus
   alaPimsmAsmFastJoin
   alaPimsmSsmFastJoin
   alaPimsmBidirFastJoin
   alaPimsmBidirSsmCompat
   alaPimsmRegisterRateLimit
alaPimGlobalConfig
   alaPimBfdStatus
   alaPimJoinPruneMsgPackingStatus
PIM-STD-MIB
pim
   pimKeepalivePeriod
   pimRegisterSuppressionTime
```

show ip pim dense

Displays the status of the various global parameters for the PIM dense mode.

show ip pim dense

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip pim dense
Status                       = enabled,
Source Lifetime              = 210,
State Refresh Interval       = 60,
State Refresh Limit Interval = 0,
State Refresh TTL            = 16,
BFD Status                   = disabled,
MoFRR Status                 = disabled,
MBR All Sources Status       = disabled,
MBR Operational Status       = enabled
```

output definitions

Status	The current global (i.e., switch-wide) status of PIM-DM. Options include **enabled** and **disabled**.
Source Lifetime	The duration of the Keepalive or Source Lifetime timer. The default value is 210.
State Refresh Interval	The time-interval, in seconds, between successive State Refresh messages originated by the router. The default value is 60.
State Refresh Limit Interval	Displays the limit at which a router will not forward the State Refresh messages, if they are received at less than the interval.
State Refresh TTL	Displays the TTL to be used in the router's originated State Refresh messages. The default value is 16.
BFD Status	Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is **enabled** or **disabled** (the default) for the PIM router.
MoFRR Status	Not supported in the current release.

output definitions (continued)

MBR All Sources Status	Indicates whether or not PIM notifies DVMRP about the routes to all multicast sources learned. Options include **enabled** (routes to all sources) or **disabled** (only routes on PIM interfaces). This status only applies when the switch is operating in the Multicast Border Router (MBR) mode.
MBR Operational Status	Indicates whether or not PIM interaction with DVMRP is **enabled** or **disabled** on a MBR switch. MBR functionality is not operationally active until both PIM and DVMRP have at least one enabled and active interface.

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; **MBR All Sources Status** and **MBR Operational Status** fields added.

Related Commands

ip pim dense admin-state	Globally enables or disables PIM-DM protocol on the switch.
ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip pim state-refresh-interval	Sets the interval between successive State Refresh messages originated by a router.
ip pim state-refresh-limit	Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.
ip pim state-refresh-ttl	Sets the Time to Live to be used in a router's originated State Refresh messages if the data packet's Time to Live is not recorded.
ip pim keepalive-period	Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
ip pim bfd-state	Enables or disables the registration of PIM with the BFD protocol.
ip pim mbr all-sources	Configures PIM to notify DVMRP of all learned routes to sources. This command only applies when the switch is operating in the Multicast Border Router mode.

MIB Objects

```
ALCATEL-IND1-PIM-MIB.mib
alaPimdmGlobalConfig
   alaPimdmAdminStatus
   alaPimRefreshInterval
   alaPimdmStateRefreshLimitInterval
   alaPimdmStateRefreshTimeToLive
   alaPimMbrAllSourcesStatus
   alaPimMbrOperStatus
alaPimGlobalConfig
   alaPimBfdStatus
PIM-STD-MIB.mib
pim
   pimKeepalivePeriod
```

show ip pim ssm group

Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.

show ip pim ssm group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- This command is supported only in the sparse mode.

Examples

```
-> show ip pim ssm group
Group Address/Prefix RP Address      Mode  Override Precedence Status
--------------------+---------------+-----+--------+----------+-------
225.0.0.0/24         0.0.0.0         ssm   false    none       enabled
```

output definitions

Group Address/Prefix	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
RP Address	A 32-bit IP address that is the Rendezvous Point (RP) for groups within the group prefix.
Mode	The PIM mode to be used for groups in this prefix. The possible values include **asm**, **ssm**, or **dm**.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim ssm group	Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
pimStaticRPTable
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPRPAddress
   pimStaticRPPimMode
   pimStaticRPOverrideDynamic
   pimStaticRPPrecedence
   pimStaticRPRowStatus
```

show ip pim dense group

Displays the static configuration of multicast group mappings for PIM-Dense Mode (DM).

show ip pim dense group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- This command is supported only on PIM dense mode.

Examples

```
-> show ip pim dense group
Group Address/Prefix RP Address      Mode  Override Precedence Status
--------------------+---------------+-----+--------+----------+-------
225.0.0.0/24         0.0.0.0         dm    false    none       enabled
```

output definitions

Group Address/Prefix	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
Mode	The PIM mode to be used for groups in this prefix. The possible values include asm, ssm, or dm.
RP Address	A 32-bit IP address that is the Rendezvous Point (RP) for groups within the group prefix.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim dense group	Creates and manages the static configuration of dense mode (DM) group mappings.
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimdmDenseGroupTable
   alaPimdmDenseGroupGrpAddress
   alaPimdmDenseGroupGrpPrefixLength
   alaPimdmDenseGroupOverrideDynamic
   alaPimdmDenseGroupPrecedence
   alaPimdmDenseGroupRowStatus
```

show ip pim neighbor

Displays a list of active PIM neighbors.

show ip pim neighbor [*ip_address***]**

Syntax Definitions

ip_address	The 32-bit IP address for the PIM neighbor.

Defaults

If a neighbor's IP address is not specified, the entire PIM neighbor table is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

To view more detailed information about a particular neighbor, specify the neighbor's IP address in the command line. Additional information will be displayed, which includes LAN Prune Delay, Override Interval, TBit field, State Refresh capable, and Designated Router option status.

Examples

```
-> show ip pim neighbor
Neighbor Address     Interface Name       Uptime      Expires    DR Priority
-----------------+-------------------+-----------+-----------+-------------
212.61.20.250          vlan-2            01h:07m:07s 00h:01m:38s 100
212.61.60.200          vlan-6            01h:07m:07s 00h:01m:38s 100
214.28.4.254           vlan-26           01h:07m:07s 00h:01m:38s 100
```

If a specific neighbor IP address is specified in the command line, *detailed information for the corresponding neighbor only* displays:

```
-> show ip pim neighbor 212.61.30.7
Neighbor IP Address        = 212.61.30.7,
Interface Name             = vlan-30,
Uptime                     = 00h:04m:14s,
Expires                    = 00h:01m:31s,
Lan Prune Delay Present    = true,
Propagation Delay          = 500,
Override Interval          = 2500,
TBit field                 = false,
Gen ID Present             = true,
Gen ID Value               = 0x79ca868e,
BiDir Capable              = false,
DR Priority Present        = true,
DR Priority                = 1,
State Refresh Capable      = true
```

output definitions

Neighbor (IP) Address	The 32-bit IP address of the active PIM neighbor.
Interface Name	The name of the interface used to reach this PIM neighbor.
Uptime	The amount of time since this PIM neighbor last became a neighbor of the local router, displayed in hours, minutes, and seconds.
Expiry time	The minimum amount of time remaining before the PIM neighbor will be aged out, displayed in hours, minutes, and seconds.
Lan Prune Delay Present	Evaluates to TRUE if this neighbor is using the Lan Prune Delay option.
Propagation Delay	The expected propagation delay between PIM routers on this network.
DR Priority Present	Evaluates to TRUE if the neighbor is using the DR Priority option.
DR Priority	The value of the Designated Router Priority from the last PIM Hello message received from this neighbor. This object is always zero if the DR Priority Present value is FALSE.
TBit field	The value of the Tbit field of the LAN prune delay option received from this neighbor. The Tbit specifies the ability of the neighbor to disable Join suppression.
Generation ID Present	Evaluates to TRUE if this neighbor is using the Generation ID option.
Generation ID Value	The value of the Generation ID from the last PIM Hello message received from the neighbor.
BiDir Capable	Evaluates to TRUE if this neighbor is using the Bidirectional-PIM Capable option.
State Refresh Capable	Displays whether the neighbor is capable of receiving State Refresh messages. Options include **true** or **false**.
Override Interval	The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim interface	Displays the PIM interface configuration.

MIB Objects

```
pimNeighborTable
   pimNeighborIfIndex
   pimNeighborAddressType
   pimNeighborAddress
   pimNeighborGenerationIDPresent
   pimNeighborGenerationIDValue
   pimNeighborUpTime
   pimNeighborExpiryTime
   pimNeighborDRPriorityPresent
   pimNeighborDRPriority
   pimNeighborLanPruneDelayPresent
   pimNeighborTBit
   pimNeighborPropagationDelay
   pimNeighborOverrideInterval
   pimNeighborBidirCapable
   pimNeighborSRCapable
```

show ip pim candidate-rp

Displays the IP multicast groups for which the local router advertises itself as a Candidate-RP.

show ip pim candidate-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip pim candidate-rp
RP Address       Group Address       Priority  Interval  Mode  Status
---------------+------------------+---------+---------+-----+---------
40.1.50.25       225.0.0.0/8         192       60        bidir enabled
```

output definitions

RP Address	A 32-bit IP address that is advertised as the Candidate-Rendezvous Point (RP).
Group Address	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash character (/). This is the group for which the local router advertises itself as a C-RP.
Priority	The C-RP router's priority. The lower the value, the higher the priority.
Interval	The time interval at which the C-RP advertisements are sent to the BSR.
Mode	Whether or not the Group Address is for a PIM-SM group or a Bidirectional PIM (BIDIR-PIM) group.
Status	The current status of this entry. The status is shown as enabled only if the PIM-SM is globally enabled and the PIM interface is enabled.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **Mode** field added.

Related Commands

ip pim candidate-rp	Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IP multicast group(s).

MIB Objects

```
pimBsrCandidateRPTable
   pimBsrCandidateRPAddressType
   pimBsrCandidateRPAddress
   pimBsrCandidateRPGroupAddress
   pimBsrCandidateRPGroupPrefixLength
   pimBsrCandidateRPBidir
   pimBsrCandidateRPAdvTimer
   pimBsrCandidateRPPriority
   pimBsrCandidateRPAdvInterval
   pimBsrCandidateRPHoldtime
   pimBsrCandidateRPStatus
   pimBsrCandidateRPStorageType
```

show ip pim group-map

Displays the PIM group mapping table.

show ip pim group-map [bsr | static-rp | ssm | dense]

Syntax Definitions

N/A

Defaults

If the keywords **bsr**, **static-rp**, **ssm**, or **dense** are included in the command line, then only the entries that were created by the specified origin are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined through the **ip pim static-rp** command. As long as the RP addresses defined in the static RP set are reachable, they will be added to the group mapping table.
- If the IP multicast groups are mapped to the mode SSM or DM, then the entries created by local SSM address range configuration using the **ip pim ssm group** command and local Dense Mode address range configuration using the **ip pim dense group** command are displayed.
- If the bootstrap mechanism is being used, this information is obtained from received Candidate-RP advertisements (when the local router is the BSR; when the local router is not the BSR, this information is obtained from received bootstrap messages).

Examples

```
-> show ip pim group-map
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+------------+-----+-----------
BSR       225.0.0.0/24                172.21.63.11  asm   192
BSR       225.0.0.0/24                214.0.0.7     asm   192
BSR       225.0.0.0/8                 40.1.50.25    bidir 192
Static RP 226.0.0.0/8                 10.11.203.8   bidir none
Static RP 232.0.0.0/8                               ssm

-> show ip pim group-map bsr
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+------------+-----+-----------
BSR       225.0.0.0/24                172.21.63.11  asm   192
BSR       225.0.0.0/24                214.0.0.7     asm   192
BSR       225.0.0.0/8                 40.1.50.25    bidir 192
```

```
-> show ip pim group-map static-rp
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
--------+--------------------------+------------+-----+-----------
Static RP 226.0.0.0/8                 10.11.203.8   bidir none
Static RP 232.0.0.0/8                               ssm
```

output definitions

Origin	The mechanism by which the PIM mode and RP for the group were learned. The possible values include 'static RP' for local static RP configuration, 'static SSM' for both SSM group configuration and Dense Mode Group configuration, and 'BSR' for the PIM Bootstrap Router mechanism.
Group Address/Prefix Length	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
RP Address	The IP address of the Rendezvous Point to be used for groups within the group prefix. There is no RP address if the PIM mode is either SSM or DM.
Mode	The PIM mode to be used for groups in this prefix.
Mapping Precedence	The precedence value of a particular row, which determines which row applies to a given group address. Numerically higher values for this object indicate lower precedences, with the value zero denoting the highest precedence.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **bidir** mode support added.

Related Commands

ip pim ssm group	Creates and manages the static configuration of a Source Specific Multicast mode group mappings.
ip pim dense group	Creates and manages the static configuration of dense mode (DM) group mappings.
ip pim static-rp	Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

MIB Objects

```
pimGroupMappingTable
   pimGroupMappingOrigin
   pimGroupMappingAddressType
   pimGroupMappingGrpAddress
   pimGroupMappingGrpPrefixLength
   pimGroupMappingRPAddressType
   pimGroupMappingRPAddress
   pimGroupMappingPimMode
   pimGroupMappingPrecedence
```

show ip pim interface

Displays detailed PIM settings for a specific interface. In general, it displays PIM settings for all the interfaces if no argument is specified.

show ip pim interface [*if_name***]**

Syntax Definitions

if_name	The interface name.

Defaults

By default, displays a summary list of IP PIM interfaces.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

To view more detailed information about a particular interface, specify the interface name in the command line. Additional information includes Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

Examples

```
-> show ip pim interface

Total 1 Interfaces

Interface Name       IP Address    Designated   Hello    J/P      Oper     BFD
                                   Router       Interval Interval Status   Status
------------------+-------------+-------------+--------+--------+--------+--------
vlan-203           11.12.203.8   11.12.203.8   30       60       disabled disabled

-> show ip pim interface vlan-203
Interface Name              = vlan-203,
IP Address                  = 11.12.203.8,
Designated Router           = 11.12.203.8,
Hello Interval              = 30,
Triggered Hello Interval    = 5,
Hello HoldTime              = 105,
Join/Prune Interval         = 60,
Join/Prune HoldTime         = 210,
Propagation (Prune) Delay   = 500,
Override Interval           = 2500,
Generation ID               = 0x53291e4c,
DR Priority                 = 1,
DR Priority Enabled         = true,
Lan Delay Enabled           = true,
Effective Propagation Delay = 500,
Effective Override Interval = 2500,
Suppression Enabled         = true,
```

```
Stub Interface              = false,
Prune Limit Interval        = 60,
Graft Retry Interval        = 3,
State Refresh Enabled       = true,
BiDir Capable               = false,
DF Election Robustness      = 3,
Operational Status          = disabled,
BFD Status                  = disabled,
Join/Prune MTU              = 1000,
Join/Prune Triggered Delay  = 100
```

output definitions

Interface Name	The name of the interface on which PIM is enabled.
IP address	Specifies the IP address of the specified interface.
Designated Router	The 32-bit IP address for the Designated Router (DR). The DR acts on behalf of any directly-connected hosts with respect to the PIM-SM protocol. Only one router in the LAN will act as the DR.
Hello Interval	The frequency at which PIM Hello messages are transmitted on a specified interface. Values may range from 1 to 18000. The default value is 30.
Triggered Hello Interval	The current Triggered Hello Interval. This value indicates the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface. Values may range from 1 to 60. The default value is 5.
Hello Holdtime	The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 105.
Join/Prune Interval	The Join/Prune interval for the associated interface. The Join/Prune interval is the interval at which periodic PIM-SM Join/Prune messages are sent. Values may range from 1 to 18000.
Join/Prune Holdtime	The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 210.
Propagation (Prune) Delay	The expected propagation delay between PIM routers on this network.
Override Interval	The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.
Generation ID	The value of the Generation ID this router inserted in the last PIM Hello message it sent on this interface.
DR Priority	Displays the Designated Router priority for each interface. This value is used in determining the Designated Router on an interface. Values may range from 1 to 192. A higher numeric value denotes a higher priority. Note that priority-based election is used only if all routers on the interface are using the DR priority option. The default value is 1.

output definitions (continued)

DR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the DR Priority option.
Lan Delay Enabled	Options include **true** and **false**. The value will be true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting will be false.
Effective Propagation Delay	The Effective Propagation Delay on this interface.
Effective Override Interval	The Effective Override Interval on this interface.
Suppression Enabled	Specifies whether the Join suppression is enabled on this interface.
Stub Interface	Specifies whether this interface is a 'stub interface'. If this is TRUE, then no PIM packets are sent out on this interface, and any received PIM packets are ignored.
Prune Limit Interval	The minimum interval that must transpire between two successive Prunes sent by a router. This is used only with PIM-DM.
Graft Retry Interval	Displays the time-interval a router waits for a Graft acknowledgment before resending a Graft on the interface. This is used only with PIM-DM. Values may range from 1 to 65535. The default value is 3.
State Refresh Enabled	Evaluates to TRUE if all routers on this interface are using the State Refresh option. This is used only by PIM-DM.
BiDir Capable	Evaluates to TRUE if all routers on this interface are using the Bidirectional Capable option. This is used only by BIDIR-PIM.
DF Election Robustness	The minimum number of PIM Designated Forwarder (DF) Election messages that must be lost to determine that the DF Election process has failed for this interface. This is used only by BIDIR-PIM.
Operational Status	The current operational status of the corresponding interface. Options include **enabled** and **disabled**. This value indicates whether the IP interface is operationally up. For example, if PIM is enabled on the interface, but the IP interface is currently down, this field will display as disabled. The default setting is **disabled**. To globally enable or disable PIM on the switch, use the **ip pim sparse admin-state** and **ip pim dense admin-state** commands.
BFD Status	Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is **enabled** or **disabled** (the default) for the PIM interface. Configured through the **ip pim interface bfd-state** command**.**
Join/Prune MTU	The configured PIM Join/Prune packet MTU for this interface.
Join/Prune Triggered Delay	The triggered Join/Prune delay.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **BiDir Capable** and **DF Election Robustness** fields added.
Release 8.6R1; **Join/Prune MTU** and **Join/Prune Triggered** Delay fields added.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceIPVersion
   pimInterfaceAddressType
   pimInterfaceAddress
   pimInterfaceGenerationIDValue
   pimInterfaceDR
   pimInterfaceDRPriority
   pimInterfaceDRPriorityEnabled
   pimInterfaceHelloInterval
   pimInterfaceTrigHelloInterval
   pimInterfaceHelloHoldtime
   pimInterfaceJoinPruneInterval
   pimInterfaceJoinPruneHoldtime
   pimInterfaceDFElectionRobustness
   pimInterfaceLanDelayEnabled
   pimInterfacePropagationDelay
   pimInterfaceOverrideInterval
   pimInterfaceEffectPropagDelay
   pimInterfaceEffectOverrideIvl
   pimInterfaceSuppressionEnabled
   pimInterfaceBidirCapable
   pimInterfaceDomainBorder
   pimInterfaceStubInterface
   pimInterfacePruneLimitInterval
   pimInterfaceGraftRetryInterval
   pimInterfaceSRPriorityEnabled
   pimInterfaceStatus
alaPimInterfaceAugTable
   alaPimInterfaceBfdStatus
   alaPimInterfaceJoinPruneMtu
   alaPimInterfaceJoinPruneDelay
```

show ip pim static-rp

Displays the PIM Static RP table for the ASM mode, which includes group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the Static RP configuration (i.e., enabled or disabled).

show ip pim static-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ip pim static-rp
Group Address/Pref Length   RP Address    Mode  Override Precedence Status
----------------------------+-------------+-----+--------+----------+--------
225.0.0.0/24                172.21.63.11  asm   false    none       enabled
226.0.0.0/8                 10.11.203.8   bidir false    none       enabled
```

output definitions

Group Address/Pref Length	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/). To change the current multicast group address and mask, refer to the **ip pim static-rp** command on page 33-15.
RP Address	A 32-bit IP address of the Rendezvous Point (RP). To change the current RP address, refer to the **ip pim static-rp** command on page 33-15.
Mode	The PIM mode to be used for groups in this prefix. The possible values include **asm**, **ssm**, or **bidir**.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).

output definitions

Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether static RP configuration is currently enabled or disabled. Options include **enabled** and **disabled**. To change the current status, refer to the **ip pim static-rp** command.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4: **bidir** mode support added.

Related Commands

ip pim static-rp	Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

MIB Objects

```
pimStaticRPTable
   pimStaticRPAddressType
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPRPAddress
   pimStaticRPPimMode
   pimStaticRPOverrideDynamic
   pimStaticRPPrecedence
   pimStaticRPRowStatus
   pimStaticRPStorageType
```

show ip pim anycast-rp

Displays the anycast RP table, which includes the anycast RP address, the RP address, if its the local router, and the current status of the anycast RP configuration.

show ip pim anycast-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ip pim anycast-rp
Anycast RP Address      Router Address     Local    Status
--------------------+------------------+--------+---------
10.10.10.1               10.1.1.2          true    enabled
10.10.10.1               10.1.2.2          false   enabled
```

output definitions

Anycast RP Address	The anycast RP address.
Router Address	The router IP address that is a member of the anycast RP set.
Local	Displays whether this entry corresponds to the local router. The value will display true if this entry corresponds to the local router and false if it does not correspond to the local router.
Status	Displays whether the anycast RP configuration is currently enabled or disabled. To change the current status, refer to the **ip pim anycast-rp** command.

Release History

Release 8.6R2; command introduced.

Related Commands

ip pim anycast-rp	Configures the anycast RP set, which is the set of all routers that would act as the RP.

MIB Objects

```
pimAnycastRPSetTable
   pimAnycastRPSetAddressType
   pimAnycastRPSetAnycastAddress
   pimAnycastRPSetRouterAddress
   pimAnycastRPSetLocalRouter
   pimAnycastRPSetRowStatus
```

show ip pim cbsr

Displays the Candidate-BSR information that is used in the Bootstrap messages.

show ip pim cbsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip pim cbsr
CBSR Address             = 214.0.0.7,
Status                   = enabled,
CBSR Priority            = 0,
Hash Mask Length         = 30,
Elected BSR              = False,
Timer                    = 00h:00m:00s
```

output definitions

CBSR Address	The 32-bit address that the local router uses to advertise itself as a Candidate-BSR.
Status	The current status of this entry. The status is shown as enabled only if the PIM-SM is globally enabled and the PIM interface is enabled.
CBSR Priority	The value for the local router as a Candidate-BSR. The higher the value, the higher the priority.
Hash Mask Length	The 32-bit mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group.
Elected BSR	Specifies whether the local router is the elected BSR.
Timer	The time value that is remaining before the local router originates the next bootstrap message. This value is zero if this router is not the elected BSR.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim cbsr	Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBSrCandidateBSRTable
   pimBsrCandidateBSRZoneIndex
   pimBsrCandidateBSRAddressType
   pimBsrCandidateBSRAddress
   pimBsrCandidateBSRPriority
   pimBsrCandidateBSRHashMaskLength
   pimBsrCandidateBSRElectedBSR
   pimBsrCandidateBSRBootstrapTimer
   pimBsrCandidateBSRStatus
```

show ip pim bsr

Displays information about the elected BSR.

show ip pim bsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip pim bsr
BSR Address              = 214.0.0.7
BSR Priority             = 192,
Hash Mask Length         = 30,
Expiry Time              = 00h:01m:35s
```

output definitions

BSR Address	The 32-bit address of the elected BSR.
BSR Priority	The priority value of the elected BSR. The higher the value, the higher the priority.
Hash Mask Length	The 32-bit mask length that is advertised in the bootstrap messages by the elected BSR (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group).
Expiry Time	The minimum time remaining before the elected BSR will be declared down.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim cbsr	Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBsrElectedBSRTable
   pimBsrElectedBSRZoneIndex
   pimBsrElectedBSRAddressType
   pimBsrElectedBSRAddress
   pimBsrElectedBSRPriority
   pimBsrElectedBSRHashMaskLength
   pimBsrElectedBSRExpiryTime
```

show ip pim notifications

Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

show ip pim notifications

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The outputs from this command includes both IPv4 and IPv6 information.

Examples

```
-> show ip pim notifications
Neighbor Loss Notifications
  Period       = 0
  Count        = 0
Invalid Register Notifications
  Period       = 65535
  Msgs Rcvd    = 0
  Origin       = None
  Group        = None
  RP           = None
Invalid Join Prune Notifications
  Period       = 65535
  Msgs Rcvd    = 0
  Origin       = None
  Group        = None
  RP           = None
RP Mapping Notifications
  Period       = 65535
  Count        = 0
Interface Election Notifications
  Period       = 65535
  Count        = 0
Non Bidir Hello Notifications
  Period      = 65535
  Msgs Rcvd   = 0
  Origin      = None
```

output definitions

Neighbor Loss Notification	**Period:** Minimum time interval that must elapse between the PIM neighbor loss notification originated by the device. **Count:** The number of neighbor loss events that have occurred. This counter is incremented whenever a neighbor loss notification is generated.
Invalid Register Notification	**Period:** Minimum time interval that must elapse between the PIM invalid register notifications originated by the device. **Msgs Rcvd:** The number of invalid PIM register notification messages that have been received by the device. **Group:** The multicast group address to which the last unexpected Register message received by the device was addressed. **RP:** The RP address to which the last unexpected Register message received by the device was delivered. **Origin**: The source address of the last unexpected Register message received by the device.
Invalid Join/Prune Notification	**Period:** Minimum time that must elapse between PIM invalid joinprune notifications originated by the device. **Msgs Rcvd:** The number of invalid PIM join/prune messages that have been received by the device. **Origin**: The source address of the last unexpected join/prune message received by the device. **Group**: The multicast group address carried in the last unexpected joinprune message received by the device. **RP**: The RP address carried in the last unexpected join/prune message received by the device.
RP Mapping Notifications	**Period**: Minimum time that must elapse between PIM RP mapping change notifications originated by the device. **Count**: The number of changes to active RP mappings on this device.
Interface Election Notifications	**Period**: Minimum time that must elapse between PIM Interface Election traps originated by the router. **Count:** The number of times this device has been elected DR on any interface.
Non Bidir Hello Notifications	**Period:** Minimum time that must elapse between notifications that the Bidirectional PIM (BIDIR-PIM) router has received a PIM Hello message from a router that is *not* a BIDIR-PIM router. **Msgs Rcvd:** The number of this type of PIM Hello messages that have been received by the router. **Origin**: The source address of the last PIM Hello message received by the device from a router that is not a BIDIR-PIM router.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **Non Bidir Hello Notifications** field added.

Related Commands

ip pim neighbor-loss-notification-period	Specifies the minimum time that must elapse between PIM neighbor loss notifications originated by the router.
ip pim invalid-register-notification-period	Specifies the minimum time that must elapse between PIM invalid register notifications originated by the router.
ip pim invalid-joinprune-notification-period	Specifies the minimum time that must elapse between PIM invalid joinprune notifications originated by the router.
ip pim rp-mapping-notification-period	Specifies the minimum time that must elapse between PIM RP mapping notifications originated by this router.
ip pim interface-election-notification-period	Specifies the minimum time that must elapse between the PIM interface election notifications originated by the router.
ip pim nonbidir-hello-notification-period	Specifies the minimum time that must elapse between notifications that the BIDIR-PIM router has received a PIM Hello message from a router that is *not* a BIDIR-PIM router.

MIB Objects

```
ALCATEL-IND1-PIM-MIB.mib
alaPimsmGlobalConfig
   alaPimsmNonBidirHelloPeriod
   alaPimsmNonBidirHelloMsgsRcvd
   alaPimsmNonBidirHelloOrigin
PIM-STD-MIB.mib
pim
   pimNeighborLossNotificationPeriod
   pimNeighborLossCount
   pimInvalidRegisterNotificationPeriod
   pimInvalidRegisterMsgsRcvd
   pimInvalidRegisterGroup
   pimInvalidRegisterRp
   pimInvalidJoinPruneNotificationPeriod
   pimInvalidJoinPruneMsgsRcvd
   pimInvalidJoinPruneOrigin
   pimInvalidJoinPruneGroup
   pimInvalidJoinPruneRP
   pimRPMappingNotificationPeriod
   pimRPMappingChangeCount
   pimInterfaceElectionNotificationPeriod
   pimInterfaceElectionWinCount
```

show ip pim groute

Displays (*,G) routing table entries for IPv4 PIM.

show ip pim groute [*group_address***]**

Syntax Definitions

group_address	A 32-bit multicast address. If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

Defaults

By default, the entire (*,G) routing table is displayed. To view more detailed (*,G) state information about a particular group, specify the group address in the command line.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

When the *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.

Examples

```
-> show ip pim groute

Total 1 (*,G)

Group Address   RP Address     RPF Interface   Upstream Neighbor UpTime      Mode
---------------+--------------+---------------+-----------------+-----------+------
225.0.0.0       212.61.60.8    vlan-30         212.61.30.7       00h:01m:43s asm
225.0.0.1       212.61.60.8    vlan-30         212.61.30.7       00h:01m:43s bidir

-> show ip pim groute 225.0.0.0
(*,225.0.0.0)
  UpTime                  = 00h:01m:49s
  RP Address              = 212.61.60.8,
  PIM Mode                = ASM,
  PIM Mode Origin         = BSR,
  Upstream Join State     = Joined,
  Upstream Join Timer     = 00h:00m:11s,
  Upstream Neighbor       = 212.61.30.7,
  RPF Interface           = vlan-30,
  RPF Next Hop            = 212.61.30.7,
  RPF Route Protocol      = OSPF,
  RPF Route Address       = 212.61.60.0/24,
  RPF Route Metric Pref   = 110,
  RPF Route Metric        = 2,
  Interface Specific State:
    vlan-4
      UpTime                    = 00h:01m:49s,
```

```
    Local Membership          = True,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-5
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-8
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-9
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-30
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
```

output definitions

Group-address	The IPv4 Multicast Group Address.
RP Address	The address of the Rendezvous Point (RP) for the group.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (*,G) join messages to.
UpTime	The time since this entry was created.
Mode	Whether this entry represents an **asm** (Any Source Multicast) or **bidir** (Bidirectional PIM) group.
Pim Mode Origin	The mechanism by which the PIM mode and RP for the group were learned.
Upstream Join State	Whether the local router should join the RP tree for the group.

output definitions (continued)

Upstream Join Timer	The time remaining before the local router next sends a periodic (*,G) Join message on the RPF IfIndex.
RPF Next Hop	The address of the RPF next hop towards the RP.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF interface towards the RP was learned.
RPF Route Address/Prefix Length	The IPv6 address combined with the prefix length identifies the route used to find the RPF interface towards the RP.
Route Metric Pref	The metric preference of the route used to find the RPF interface towards the RP.
Route Metric	The routing metric of the route used to find the RPF interface towards the RP.
Interface Name	The interface name that corresponds to the ifIndex.
Local Membership	Whether the local router has (*,G) local membership on this interface.
Join Prune State	The state resulting from (*,G) Join/Prune messages received on this interface.
Prune Pending Timer	The time remaining before the local router acts on a (*,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.
Join Expiry Timer	The time remaining before (*,G) Join state for this interface expires.
Assert State	The (*,G) Assert state for this interface. The possible values are No Info, Winner, or Loser.
Assert Timer	If Assert State is 'Winner', this is the time remaining before the local router next sends a (*,G) Assert message on this interface. If the Assert State is 'Loser', this is the time remaining before the (*,G) assert state expires.
Assert Winner Address	If the Assert State is 'Loser', this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is 'Loser', this is the metric preference of the route to the RP advertised by the assert winner; otherwise, this is zero.
Assert Winner Metric	If the Assert State is 'Loser', this is the routing metric of the route to the RP advertised by the assert winner; otherwise, this is zero.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; Mode field added, **bidir** mode support added

Related Commands

show ip pim sgroute	Displays (S,G) state routing table entries.

MIB Objects

pimStarGTable

- pimStarGAddressType
- pimStarGGrpAddress
- pimStarGUpTime
- pimStarGPimMode
- pimStarGRPAddressType
- pimStarGRPAddress
- pimStarGPimModeOrigin
- pimStarGRPIsLocal
- pimStarGUpstreamJoinState
- pimStarGUpstreamJoinTimer
- pimStarGUpstreamNeighborType
- pimStarGUpstreamNeighbor
- pimStarGRPFIfIndex
- pimStarGRPFNextHopType
- pimStarGRPFNextHop
- pimStarGRPFRouteProtocol
- pimStarGRPFRouteAddress
- pimStarGRPFRoutePrefixLength
- pimStarGRPFRouteMetricPref
- pimStarGRPFRouteMetric

pimStarGITable

- pimStarGIIfIndex
- pimStarGIUpTime
- pimStarGILocalMembership
- pimStarGIJoinPruneState
- pimStarGIPrunePendingTimer
- pimStarGIJoinExpiryTimer
- pimStarGIAssertState
- pimStarGIAssertTimer
- pimStarGIAssertWinnerAddressType
- pimStarGIAssertWinnerAddress
- pimStarGIAssertWinnerMetricPref
- pimStarGIAssertWinnerMetric

show ip pim sgroute

Displays (S,G) routing table entries for IPv4 PIM.

show ip pim sgroute [*source_address group_address***]**

Syntax Definitions

source_address	The 32-bit IP address for a specific multicast source.
group_address	A 32-bit multicast address.

Defaults

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the *source_address* and *group_address* associated with that entry.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the *source_address* and *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

Examples

```
-> show ip pim sgroute
Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
               L = Local, R = RPT, T = SPT, F = Register,
               P = Pruned, O = Originator
Total 1 (S,G)

Source Address Group Address RPF Interface  Upstream Neighbor UpTime      Flags
--------------+-------------+--------------+-----------------+-----------+--------
172.21.63.2    225.0.0.0     vlan-30        212.61.30.7       00h:02m:09s ST
172.21.63.2    225.0.0.1     vlan-30        212.61.30.7       00h:02m:09s ST


-> show ip pim sgroute 172.21.63.2 225.0.0.0
(172.21.63.2,225.0.0.0)
  UpTime                  = 00h:02m:16s
  PIM Mode                = ASM,
  Upstream Join State     = Joined,
  Upstream RPT State      = Not Pruned,
  Upstream Join Timer     = 00h:00m:44s,
  Upstream Neighbor       = 212.61.30.7,
  RPF Interface           = vlan-30,
  RPF Next Hop            = 212.61.30.7,
  RPF Route Protocol      = OSPF,
  RPF Route Address       = 172.21.63.0/24,
  RPF Route Metric Pref   = 110,
  RPF Route Metric        = 2,
```

```
SPT Bit                 = True,
DR Register State       = No Info,
DR Register Stop Timer  = 00h:00m:00s,
Interface Specific State:
  vlan-4
    UpTime                    = 00h:02m:16s,
    Local Membership          = True,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-5
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-8
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-9
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-30
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    RPT State                 = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
```

output definitions

Source-address	The IPv4 Source address.
Group-address	The IPv4 Multicast Group Address.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.

output definitions (continued)

Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (S,G) join messages to.
UpTime	The time since this entry was created.
Flags	Flags indicating SPTBit, Prune State, Join State, etc.
Pim Mode	Whether the Group Address is SSM, ASM or DM.
Upstream Join State	Whether the local router should join the SPT for the source and group represented by this entry.
Upstream Join Timer	The time remaining before the local router next sends a periodic (S,G) Join message.
RPF Next Hop	The address of the RPF next hop towards the source.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF Interface towards the source was learned.
RPF Route Address/Prefix Length	The IP address which when combined with the Route Prefix length identifies the route used to find the RPF interface towards the source.
RPF Route Metric Pref	The metric preference of the route used to find the RPF interface towards the source.
RPF Route Metric	The metric preference of the route used to find the RPF interface towards the source.
DR Register State	Whether the local router should encapsulate (S,G) data packets in Register messages and send them to the RP. The possible values include No Info, Join, Join Pending, or Prune.
DR Register Stop Timer	The value of the Register Stop Timer. If the Register State is 'prune', this is the time remaining before the local router sends a Null-Register message to the RP. If the State is 'joinPending', this is the time remaining before the local router resumes encapsulating data packets and sending them to the RP.
Upstream Prune State	Whether the local router has pruned itself from the tree. This is only used by PIM-DM. The possible values include forwarding, Ack Pending, or Pruned.
Upstream Prune Limit Timer	The time remaining before the local router may send a (S,G) prune message on alaPimSGRPFIfIndex. This is only used by PIM-DM.
Originator State	Whether this router is an originator for the (S,G) message flow. This is only used by PIM-DM. The possible values include Not Originator or Originator.
Source Active Timer	If this router is the Originator, this is the time remaining before the local router reverts to notOriginator state. Otherwise, this is zero. This is only used by PIM-DM.
State Refresh Timer	If Originator state is 'originator', this is the time remaining before the local router sends a State Refresh Message. Otherwise, this is zero. This is only used by PIM-DM.
Interface Name	The interface name corresponding to the ifIndex that corresponds to this entry.
Uptime	The time since this entry was created.
Local Membership	Whether the local router has (S,G) local membership on this interface.

output definitions (continued)

Join Prune State	The state resulting from (S,G) Join/Prune messages received on this interface. The possible values include No Info, Join, or Prune Pending.
Prune Pending Timer	The time remaining before the local router acts on an (S,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.
Join Expiry Timer	The time remaining before (S,G) Join state for this interface expires.
Assert State	The (S,G) Assert state for this interface. The possible values include No Info, Winner, or Loser.
Assert Timer	If Assert State is Winner, this is the time remaining before the local router sends a (S,G) Assert message on this interface. If the Assert State is Loser, this is the time remaining before the (S,G) Assert state expires.
Assert Winner	If the Assert State is Loser, this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is Loser, this is the metric preference of the route to the source advertised by the assert winner.
Assert Winner Metric Metric	If the Assert State is Loser, this is the routing metric of the route to the source advertised by the assert winner.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim groute	Displays (*,G) routing table entries for IPv4 PIM.

MIB Objects

```
pimSGTable
   pimSGAddressType
   pimSGGrpAddress
   pimSGSrcAddress
   pimSGUpTime
   pimSGPimMode
   pimSGUpstreamJoinState
   pimSGUpstreamJoinTimer
   pimSGUpstreamNeighbor
   pimSGRPFIfIndex
   pimSGRPFNextHopType
   pimSGRPFNextHop
   pimSGRPFRouteProtocol
   pimSGRPFRouteAddress
   pimSGRPFRoutePrefixLength
   pimSGRPFRouteMetricPref
   pimSGRPFRouteMetric
   pimSGSPTBit
   pimSGKeepaliveTimer
   pimSGDRRegisterState
   pimSGDRRegisterStopTimer
   pimSGRPRegisterPMBRAddressType
   pimSGRPRegisterPMBRAddress
```

```
   pimSGUpstreamPruneState
   pimSGUpstreamPruneLimitTimer
   pimSGOriginatorState
   pimSGSourceActiveTimer
   pimSGStateRefreshTimer
pimSGITable
   pimSGIIfIndex
   pimSGIUpTime
   pimSGILocalMembership
   pimSGIJoinPruneState
   pimSGIPrunePendingTimer
   pimSGIJoinExpiryTimer
   pimSGIAssertState
   pimSGIAssertTimer
   pimSGIAssertWinnerAddressType
   pimSGIAssertWinnerAddress
   pimSGIAssertWinnerMetricPref
   pimSGIAssertWinnerMetric
```

show ip pim df-election

Displays the Designated Forwarder (DF) election state for Rendezvous Point (RP) interfaces. This command applies only to RPs operating in the Bidirectional PIM (BIDIR-PIM) mode.

show ip pim df-election [*rp_address* | *if_name***]**

Syntax Definitions

rp_address	A 32-bit RP address.
if_name	The interface name.

Defaults

By default, the DF election state for all RP interfaces.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the *rp_address* is specified in the command line, only those interfaces associated with the specified RP address are displayed.
- When the *if_name* is specified in the command line, only information associated with the specified interface is displayed.

Examples

```
-> show ip pim df-election
RP Address  Interface Name DF State Winner Address Uptime      Metric  Metric Expires
                                                               Pref
-----------+--------------+--------+-------------+-----------+-------+------+----------
10.11.203.8 vlan-13        Win      10.11.126.3    00h:06m:31s 1       1     00h:00m:24s
            vlan-200       Win      10.11.200.1    00h:06m:31s 1       1     00h:00m:24s
            vlan-204       Win      10.11.204.8    00h:06m:31s 1       1     00h:00m:24s
            vlan-210       Win      10.5.5.8       00h:06m:31s 1       1     00h:00m:24s
40.1.50.25  vlan-203       Lose     10.11.203.27   00h:00m:22s 1       1     00h:00m:00s
            vlan-13        Win      10.11.126.3    00h:06m:31s 110     2     00h:00m:32s
            vlan-200       Win      10.11.200.1    00h:06m:31s 110     2     00h:00m:32s
            vlan-204       Lose     10.11.204.27   00h:00m:22s 1       1     00h:00m:00s
            vlan-210       Win      10.5.5.8       00h:06m:31s 110     2     00h:00m:32s

-> show ip pim df-election 40.1.50.25
RP Address  Interface Name DF State Winner Address Uptime      Metric  Metric Expires
                                                               Pref
-----------+--------------+--------+-------------+-----------+-------+------+----------
40.1.50.25  vlan-203       Lose     10.11.203.27   00h:00m:22s 1       1     00h:00m:00s
            vlan-13        Win      10.11.126.3    00h:06m:31s 110     2     00h:00m:32s
            vlan-200       Win      10.11.200.1    00h:06m:31s 110     2     00h:00m:32s
            vlan-204       Lose     10.11.204.27   00h:00m:22s 1       1     00h:00m:00s
            vlan-210       Win      10.5.5.8       00h:06m:31s 110     2     00h:00m:32s
```

```
-> show ip pim df-election vlan-200
RP Address  Interface Name DF State Winner Address Uptime      Metric  Metric Expires
                                                              Pref
-----------+--------------+--------+--------------+-----------+-------+------+----------
10.11.203.8 vlan-200       Win      10.11.200.1    00h:06m:31s 1       1     00h:00m:24s
40.1.50.25  vlan-200       Win      10.11.200.1    00h:06m:31s 110     2     00h:00m:32s
```

output definitions

RP Address	The IPv4 address of the Rendezvous Point (RP).
Interface Name	The name of the IPv4 interface.
DF State	The state of the DF election process (**Offer**, **Lose**, **Win**, or **Backoff**).
Winner Address	The primary IPv4 address of the winner of the DF election process.
UpTime	The amount of time since the current winner was last elected the DF for the RP.
Metric Pref	The metric preference advertised by the DF winner. This value is zero if there currently is no DF.
Metric	The metric value advertised by the DF winner. This value is zero if there currently is no DF.
Expires	The minimum time remaining before the local router expires the current DF state.

Release History

Release 7.3.4; command was introduced.

Related Commands

show ip pim interface	Displays detailed PIM settings for a specific interface.

MIB Objects

```
pimBidirDFElectionTable
   pimBidirDFElectionAddressType
   pimBidirDFElectionRPAddress
   pimBidirDFElectionIfIndex
   pimBidirDFElectionWinnerAddressType
   pimBidirDFElectionWinnerAddress
   pimBidirDFElectionWinnerUpTime
   pimBidirDFElectionWinnerMetricPref
   pimBidirDFElectionWinnerMetric
   pimBidirDFElectionState
   pimBidirDFElectionStateTimer
```

ipv6 pim sparse admin-state

Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.

ipv6 pim sparse admin-state {enable | disable}

Syntax Definitions

enable	Enables PIM-SM globally for IPv6.
disable	Disables PIM-SM globally for IPv6.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command must be set to **enable** before PIM-SM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 33-3 for more information.

Examples

```
-> ipv6 pim sparse admin-state enable
-> ipv6 pim sparse admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6AdminStatus
```

ipv6 pim bidir admin-state

Enables or disables IPv6 BIDIR-PIM (bidirectional) globally for IPv6.

ipv6 pim bidir admin-state {enable | disable}

Syntax Definitions

enable	Enables BIDIR-PIM globally for IPv6.
disable	Disables BIDIR-PIM globally for IPv6.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command must be set to **enable** before BIDIR-PIM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 33-3 for more information.

Examples

```
-> ipv6 pim bidir admin-state enable
-> ipv6 pim bidir admin-state disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

ipv6 pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6BidirStatus
```

ipv6 pim dense admin-state

Enables or disables the IPv6 PIM-DM (dense mode) globally for IPv6.

ipv6 pim dense admin-state {enable | disable}

Syntax Definitions

enable	Enables PIM-DM globally for IPv6.
disable	Disables PIM-DM globally for IPv6.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

This command must be set to **enable** before PIM-DM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 33-3 for more information.

Examples

```
-> ipv6 pim dense admin-state enable
-> ipv6 pim dense admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
   alaPimdmV6AdminStatus
```

ipv6 pim ssm group

Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

ipv6 pim ssm group *group_address/prefix_length* **[[no] override] [priority** *priority***]**

no ipv6 pim ssm group *group_address/prefix_length*

Syntax Definitions

group_address	Specifies the IPv6 multicast group address.
/prefix_length	Specifies the prefix length of the IPv6 multicast group. Values may range from 4 to 128.
override	Specifies the static SSM mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
priority	Specifies the preference value to be used for this static SSM mode configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a Source Specific Multicast mode group mapping.
- The IPv6 PIM Source-Specific Multicast (SSM) mode for the default SSM address range (FF3x::/32) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM.
- You can also map additional IPv6 multicast address ranges for the SSM group using this command. However, the IPv6 multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to unset the priority.

Examples

```
-> ipv6 pim ssm group ff30::1234:abcd/128 priority 50
-> no ipv6 pim ssm group ff30::1234:abcd/128
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim group-map	Displays the IPv6 PIM group mapping table.
show ipv6 pim ssm group	Displays the static configuration of IPv6 multicast group mappings for PIM-Source Specific Multicast (SSM).

MIB Objects

```
pimStaticRPTable
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPPimMode
   pimStaticRPPrecedence
   pimStaticRPOverrideDynamic
   pimStaticRPRowStatus
```

ipv6 pim dense group

Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

ipv6 pim dense group *group_address/prefix_length* **[[no] override] [priority** *priority***]**

no ipv6 pim dense group *group_address/prefix_length*

Syntax Definitions

group_address	Specifies the IPv6 multicast group address.
/prefix_length	Specifies the prefix length of the IPv6 multicast group.
override	Specifies the static dense mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
priority	Specifies the preference value to be used for this static configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a dense mode group mapping.
- This command specifies the mode as Dense (PIM-DM) for the specified IPv6 multicast group addresses.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to unset the priority.

Examples

```
-> ipv6 pim dense group ff0e::1234/128 priority 50
-> no ipv6 pim dense group ff0e::1234/128
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim group-map	Displays the IPv6 PIM group mapping table.
show ipv6 pim dense group	Displays the static configuration of IPv6 multicast group mappings for PIM Dense Mode (DM).

MIB Objects

```
alaPimdmDenseGroupTable
   alaPimdmDenseGroupGrpAddress
   alaPimdmDenseGroupGrpPrefixLength
   alaPimdmDenseGroupOverrideDynamic
   alaPimdmDenseGroupPrecedence
   alaPimdmDenseGroupRowStatus
```

ipv6 pim cbsr

Configures the local router as the Candidate-BSR for the PIM domain.

ipv6 pim cbsr *ipv6_address* **[priority** *priority***] [mask-length** *bits***]**

no ipv6 pim cbsr *ipv6_address*

Syntax Definitions

ipv6_address	The IPv6 unicast address that the local router will use to advertise itself as a Candidate-BSR. The specified address must be a domain-wide reachable address.
priority	The priority value of the local router as a Candidate-BSR. Values may range from 0 to 255.
bits	The hash mask length that is advertised in the bootstrap messages for IPv6 PIM (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group). Values may range from 1 to 128.

Defaults

parameter	default
priority	64
bits	126

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a Candidate-BSR for a PIM domain.
- This command is supported only in the sparse mode.
- The information configured using this command is used in the Bootstrap messages.
- Candidate-BSRs also avoid a single point of failure in a PIM domain.

Examples

```
-> ipv6 pim cbsr 2000::1 priority 100 mask-length 4
-> no ipv6 pim cbsr 2000::1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim cbsr	Displays the IPv6 Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBsrCandidateBSRTable
   pimBsrCandidateBSRAddress
   pimBsrCandidateBSRPriority
   pimBsrCandidateBSRHashMaskLength
   pimBsrCandidateBSRRowStatus
```

ipv6 pim static-rp

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

ipv6 pim static-rp *group_address/prefix_length rp_address* **[[no] bidir] [[no] override] [priority** *priority***]**

no ipv6 pim static-rp *group_address/prefix_length rp_address*

Syntax Definitions

group_address	Specifies the IPv6 multicast group address.
/prefix_length	Specifies the prefix length of the IPv6 multicast group.
rp_address	Specifies the IPv6 unicast address of the Rendezvous Point (RP). This must be a domain-wide reachable address.
bidir	Creates the static RP entry for use in the Bidirectional PIM (BIDIR-PIM) mode.
override	Specifies the static RP configuration to override the dynamically learned RP information for the specified group(s).
priority	Specifies the preference value to be used for this static RP configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the **priority** option is not set, the **override** option is set to false, and the **bidir** option is set to false.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a static RP configuration.
- Specifying the priority value obsoletes the **override** option.
- If the **bidir** parameter option is not specified with this command, the static RP entry is created for use in the ASM mode.
- The IPv6 PIM Source-Specific Multicast (SSM) mode for the default SSM address range (FF3x::/32) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM. You can also map additional IPv6 multicast address ranges for the SSM group. However, the IPv6 multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Note that once the priority option has been defined a value of 65535 can be used to unset the priority

- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim static-rp ff0e::1234/128 2000::1 priority 10
-> ipv6 pin static-rp ff0e::1234/128 2000::1 bidir overide
-> no ipv6 pim static-rp ff0e::1234/128 2000::1
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **bidir** parameter added.

Related Commands

show ipv6 pim group-map	Displays the IPv6 PIM group mapping table.
show ipv6 pim static-rp	Displays the IPv6 PIM Static RP table, which includes IPv6 multicast group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the Static RP configuration (i.e., enabled or disabled).

MIB Objects

```
pimStaticRPTable
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPRPAddress
   pimStaticRPPimMode
   pimStaticRPOverrideDynamic
   pimStaticRPPrecedence
   pimStaticRPRowStatus
```

ipv6 pim anycast-rp

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

ipv6 pim anycast-rp *anycast_rp_address rp_address*

no ipv6 pim anycast-rp *anycast_rp_address rp_address*

Syntax Definitions

anycast-rp-address	Specifies the anycast RP address.
rp_address	Specifies the IPv6 unicast address of the Rendezvous Point (RP) address of a router that is a member of the anycast RP set.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the no form of this command to delete an anycast RP configuration.
- The RP specified by anycast-RP-address is the RP in the anycast RP set. This address must be the same as the RP address in the Static-RP configuration used with the **ipv6 pim static-rp** command if static RP configuration is being used.
- It is recommended not to use Loopback0 as the anycast RP address since Loopback0 is often used as the Router ID by default with the unicast routing protocols. Hence, it is recommended. to use one of the additional LoopbackX interfaces for the anycast RP address, but it is not mandatory to be a LoopbackX address.
- The RP specified by rp-address defines the IP address of the prospective RP. This address must be different than the anycast RP address and is used in communication between the different RPs in the anycast RP set. This configuration must be the same on all routers in the Anycast-RP set.
- There must be a separate entry for each of the RPs participating in anycast RP set, including an entry for the local router.This configuration defining the anycast RP set must be the same on all routers participating in anycast RP.
- It is recommended to configure PIM register rate limiting (see **ipv6 pim register-rate-limit**) to limit the sending of PIM register messages with Anycast RP.
- Ensure SPT is enabled (see **ipv6 pim spt admin-state**) when using Anycast RP. If SPT is globally disabled, and Anycast RP configuration is added, this configuration will be ignored for all groups that are operating in Anycast-RP mode.

Examples

```
-> ipv6 pim static-rp ff00::/8 2001:1::1
```

```
-> ipv6 pim anycast-rp 2001:1::1 3001:1::1
-> ipv6 pim anycast-rp 2001:1::1 3001:1::2
-> no ipv6 pim anycast-rp 2001:1::1 3001:1::2
```

Release History

Release 8.6R2; command introduced.

Related Commands

ipv6 pim static-rp	Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).
show ipv6 pim anycast-rp	Displays the anycast RP table, which includes the anycast RP address, the RP address, if its the local router, and the current status of the anycast RP configuration.

MIB Objects

```
pimAnycastRPSetTable
   pimAnycastRPSetAddressType
   pimAnycastRPSetAnycastAddress
   pimAnycastRPSetRouterAddress
   pimAnycastRPSetRowStatus
```

ipv6 pim candidate-rp

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IPv6 multicast group(s).

ipv6 pim candidate-rp *rp_address group_address/prefix_length* **[[no] bidir] [priority** *priority***] [interval** *seconds***]**

no ipv6 pim candidate-rp *rp_address group_address/prefix_length*

Syntax Definitions

rp_address	Specifies the IPv6 unicast address that will be advertised as a Candidate-RP. This must be a domain-wide reachable address.
group_address	Specifies the IPv6 multicast group address for which the local router will advertise itself as a Candidate-RP.
/prefix_length	Specifies the prefix length of the specified IPv6 multicast group address.
bidir	Creates a C-RP entry for use in the Bidirectional PIM (BIDIR-PIM) mode.
priority	Specifies the priority value of the Candidate-RP. Values may range from 0 to 192. The lower the value, the higher the priority.
seconds	Specifies the interval at which the C-RP advertisements are sent to the bootstrap router, in seconds. Values may range from 1 to 300.

Defaults

parameter	default
[no] bidir	no bidir
priority	192
seconds	60

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a C-RP for a particular multicast group.
- Only one RP address is supported per switch. If multiple candidate-RP entries are defined, they must specify the same *rp-address.*
- If the **bidir** parameter option is not specified with this command, the C-RP entry is created for use in the ASM mode.
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim candidate-rp 2000::1 ff0e::1234/128 priority 100 interval 100
-> ipv6 pim candidate-rp 2000::1 ff0e::1234/128 bidir priority 100 interval 100
-> no ipv6 pim candidate-rp 2000::1 ff0e::1234/128
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **bidir** parameter added.

Related Commands

show ipv6 pim candidate-rp	Displays the IPv6 multicast groups for which the local router will advertise itself as a Candidate-RP.

MIB Objects

```
pimBsrCandidateRPTable
   pimBsrCandidateRPAddress
   pimBsrCandidateRPGroupAddress
   pimBsrCandidateRPGroupPrefixLength
   pimBsrCandidateRPBidir
   pimBSrCandidateRPPriority
   pimBsrCandidateRPAdvInterval
   pimBsrCandidateRPRowStatus
```

ipv6 pim rp-switchover

Enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated packet in the IPv6 PIM domain.

ipv6 pim rp-switchover {enable | disable}

Syntax Definitions

enable	Enables the RP to switch to native forwarding.
disable	Disables the RP from switching to native forwarding.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- You cannot specify a pre-configured threshold, such as the RP threshold, as you would do for IPv4 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim rp-switchover enable
-> ipv6 pim rp-switchover disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6RPSwitchover
```

ipv6 pim register-rate-limit

Configures the maximum number of PIM Register Packets that the Designated Router (DR) will send per second for each (S,G) entry.

ipv6 pim register-rate-limit *pps*

Syntax Definitions

pps	The per (S,G) register rate limit in packets per second (0–65535).

Defaults

By default, the register rate limit is set to zero.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Setting the register rate limit to zero (the default) disables register rate limiting.
- Rate limiting is applied on a per (S,G) flow basis.
- This command is supported in both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim register-rate-limit 100
-> ipv6 pim register-rate-limit 0
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfigTable
   alaPimsmV6RegisterRateLimit
```

ipv6 pim spt admin-state

Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT).

ipv6 pim spt admin-state {enable | disable}

Syntax Definitions

enable	Enables last hop DR switching to the SPT.
disable	Disables last hop DR switching to the SPT.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command is supported only in the sparse mode.
- If the SPT status is enabled, last hop DR switching to the SPT begins once the first data packet is received.

Examples

```
-> ipv6 pim spt admin-state enable
-> ipv6 pim spt admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6SPTConfig
```

ipv6 pim interface

Enables IPv6 PIM and configures the statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the IPv6 interface.

ipv6 pim interface *if_name*
[hello-interval *seconds***]**
[triggered-hello *seconds***]**
[joinprune-interval *seconds***]**
[hello-holdtime *seconds***]**
[joinprune-holdtime *seconds***]**
[prune-delay *milliseconds***]**
[override-interval *milliseconds***]**
[dr-priority *priority***]**
[prune-limit-interval *seconds***]**
[graft-retry-interval *seconds***]**
[df-election-robustness *messages***]**
[[no] stub]
[joinprune-mtu *bytes***]**
[joinprune-delay *milliseconds***]**

no ipv6 pim interface *if_name*

Syntax Definitions

if_name	The interface name on which the IPv6 PIM is being enabled or disabled.
hello-interval *seconds*	The frequency at which IPv6 PIM Hello messages are transmitted on this interface, in seconds. Values may range from 0 to 18000.
triggered-hello *seconds*	Specifies the maximum time, in seconds, before a triggered IPv6 PIM Hello message is sent on this interface. Values may range from 0 to 60.
joinprune-interval *seconds*	The frequency at which periodic IPv6 PIM Join/Prune messages are sent on this interface, in seconds. Values may range from 0 to 18000.
hello-holdtime *seconds*	Specifies the value of the IPv6 PIM hello-holdtime for this interface. This value is set in the Holdtime field of IPv6 PIM Hello messages sent on this interface, in seconds. Values may range from 0 to 65535.
joinprune-holdtime *seconds*	Specifies the value that is set in the Holdtime field of the IPv6 PIM Joinprune messages sent on this interface, in seconds.Values may range from 0 to 65535.
prune-delay *milliseconds*	Specifies the value of the expected propagation delay between IPv6 PIM routers on this network, inserted into the LAN prune-delay option of the IPv6 PIM Hello messages sent on this interface, in milliseconds. Values may range from 0 to 32767.
override-interval *milliseconds*	Specifies the value set in the Override Interval field of the LAN prune-delay option of the IPv6 PIM Hello messages sent on this interface, if the prune-delay status is enabled, in *milliseconds.* Values may range from 0 to 65535.

dr-priority *priority*	Specifies the Designated Router priority set in the DR priority option on this interface. The DR priority option value (1–192). A higher numeric value denotes a higher priority.
prune-limit-interval *seconds*	Specifies the minimum interval that must elapse between two successive IPv6 PIM prune messages sent on this interface, in seconds. Values may range from 0 to 65535.
graft-retry-interval *seconds*	Specifies the minimum interval that must elapse between two successive IPv6 PIM graft messages sent on this interface, in seconds. Values may range from 0 to 65535.
df-election-robustness *messages*	The minimum number of DF-Election messages that must be lost in order for the DF Election to fail on the specified interface. Values may range from 1–65535. This value is used only by BIDIR-PIM.
stub	Specifies the interface not to send any IPv6 PIM packets through this interface, and to ignore received IPv6 PIM packets.
joinprune-mtu *bytes*	Specifies the maximum size used for PIM Join/Prune packets getting sent out this interface. Values may range from 0 to 9198.
joinprune-delay *milliseconds*	Specifies the Join/Prune delay interval in milliseconds. Values may range from 0 to 32767.

Defaults

parameter	default
hello-interval *seconds*	30
triggered-hello *seconds*	5
joinprune-interval *seconds*	60
hello-holdtime *seconds*	105
joinprune-holdtime *seconds*	210
prune-delay *milliseconds*	500
override-interval *milliseconds*	2500
dr-priority *priority*	1
prune-limit-interval *seconds*	60
graft-retry-interval *seconds*	3
df-election-robustness *messages*	3
stub	Disabled
joinprune-mtu *bytes*	0
joinprune-delay *milliseconds*	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete an IPv6 PIM interface.

- IPv6 PIM must be enabled globally on the switch before IPv6 PIM will begin running on the interface. To globally enable or disable IPv6 PIM-SM on the switch, refer to the **ipv6 pim sparse admin-state** command on page 33-106. To enable or disable IPv6 PIM-DM on the switch, refer to the **ipv6 pim dense admin-state** command on page 33-108.
- Specifying zero for IPv6 PIM hello-interval represents an infinite time, in which case the periodic IPv6 PIM hello messages are not sent.
- Specifying zero for IPv6 PIM joinprune-interval represents an infinite time, in which case the periodic IPv6 PIM joinprune messages are not sent.
- Specifying the value of 65535 for IPv6 PIM hello-holdtime represents an infinite time. If an IPv6 PIM router gets IPv6 PIM Hello packet from a neighbor with its hello-holdtime value as infinite time, then the router will not time out the sender(neighbor). It is recommended that you use an IPv6 PIM hello-holdtime interval that is 3.5 times the value of the IPv6 PIM hello-interval, or 65535 seconds if the IPv6 PIM hello-interval is set to zero
- Specifying the value of 65535 for IPv6 PIM joinprune-holdtime represents an infinite time. The receipt of IPv6 Join/Prune messages with its joinprune-holdtime value as infinite time, then this specifies an infinite holdtime for the particular IPv6 join/prune message. It is recommended that you use a joinprune- holdtime interval that is 3.5 times the value of the IPv6 PIM Join/Prune interval defined for the interface, or 65535 seconds if the IPv6 PIM joinprune-interval is set to zero.
- The interface configured as a **stub** will not send any IPv6 PIM packets through that interface, and any received IPv6 PIM packets are also ignored. By default, an IPv6 PIM interface is not set to be a stub.
- The IPv6 PIM **graft-retry-interval** and **prune-limit-interval** options can be used only with the IPv6 PIM-DM mode.
- If the IPv6 interface on which PIM is enabled is bound to an SPB service, then PIM can operate over an SPB L3 VPN in-line routing configuration (supported only on the OmniSwitch 9900).
- By default, **joinprune-mtu** value is ‘0’ and the configured interface MTU value will be used in determining the maximum packet size that can be used in sending the packed messages. However, if the Join/Prune MTU configuration is specified, the actual maximum size used for PIM Join/Prune messages will be the smaller of the IP MTU value of the interface and the configured interface Join/ Prune MTU value.
- The **joinprune-delay** interval is used to delay the sending of triggered Join/Prune messages and may be desirable to allow the packing of triggered Join.Prune messages due to bursts of protocol messages, which may result in subsequent bursts of triggered Join/Prune packets. The default value of ‘0’ implies no deferred processing and will result in no packing of triggered Join/Prune packets.

Examples

```
-> ipv6 pim interface vlan-2 hello-interval 100 triggered-hello 10 joinprune-
interval 100 hello-holdtime 350 joinprune-holdtime 400
-> no ipv6 pim interface vlan-2
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4: **df-election robustness** parameter added.
Release 8.6R1; **joinprune-mtu**, **joinprune-delay** parameters added.

Related Command

show ipv6 pim interface	Displays detailed IPv6 PIM settings for a specific interface.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceStatus
   pimInterfaceHelloInterval
   pimInterfaceTrigHelloInterval
   pimInterfaceJoinPruneInterval
   pimInterfaceHelloHoldtime
   pimInterfaceJoinPruneHoldtime
   pimInterfaceDFElectionRobustness
   pimInterfacePropagationDelay
   pimInterfaceOverrideInterval
   pimInerfaceDRPriority
   pimInterfaceStubInterface
   pimInterfacePruneLimitInterval
   pimInterfaceGraftRetryInterval
alaPimInterfaceAugTable
   alaPimInterfaceJoinPruneDelay
   alaPimInterfaceJoinPruneMtu
```

ipv6 pim bfd-state

Enables or disables the registration of IPv6 PIM with the BFD protocol.

ipv6 pim bfd-state {enable | disable}

Syntax Definitions

enable	Enables BFD for IPv6 PIM.
disable	Disables BFD for IPv6 PIM.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- BFD must be globally enabled for the switch and PIM must be registered with BFD at the protocol level before PIM can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and PIM acts based upon the BFD message.
- Whenever a neighbor goes down, PIM will inform BFD to remove that neighbor from the BFD active list.

Examples

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of IPv6 PIM with the BFD protocol:

```
-> ipv6 pim bfd-state enable
-> ipv6 pim bfd-state disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ip bfd admin-state	Enables or disables the global BFD protocol status for the switch.
ipv6 pim bfd-state all-interfaces	Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.
ipv6 pim interface bfd-state	Enables or disables BFD monitoring on a specific PIM interface.
show ipv6 pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim dense	Displays the status of the various global parameters for the PIM dense mode.

MIB Objects

```
alaPimGlobal
   alaPimBfdStatus
```

ipv6 pim bfd-state all-interfaces

Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.

ipv6 pim bfd-state all-interfaces {enable | disable}

Syntax Definitions

enable	Enables BFD for all the IPv6 PIM interfaces.
disable	Disables BFD for all the IPv6 PIM interfaces.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The BFD status for PIM must be enabled before PIM can interact with BFD.

Examples

```
-> ipv6 pim bfd-state all-interfaces enable
-> ipv6 pim bfd-state all-interfaces disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 pim bfd-state	Enables or disables the registration of PIM with the BFD protocol.
ipv6 pim interface bfd-state	Enables or disables BFD monitoring on a specific PIM interface.
show ipv6 pim interface	Displays detailed PIM settings for a specific interface.

MIB Objects

```
alaPimGlobalConfig
   alaPimBfdAllInterfaceStatus
```

ipv6 pim interface bfd-state

Enables or disables BFD monitoring for a specific PIM interface.

ipv6 pim interface *if_name* **bfd-state {enable | disable}**

Syntax Definitions

if_name	The name of an existing IPv6 PIM interface.
enable	Enables BFD for the specified PIM interface.
disable	Disables BFD for the specified PIM interface.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Registering PIM with BFD is required at the protocol level before PIM can interact with BFD.
- When BFD is enabled on the specified PIM interface, BFD monitors the connectivity to all neighbors known through the specified interface.

Examples

```
-> ipv6 pim interface pimInt1 bfd-state enable
-> ipv6 pim interface pimInt1 bfd-state disable
```

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 pim bfd-state	Enables or disables the registration of PIM with the BFD protocol.
ipv6 pim bfd-state all-interfaces	Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.
show ipv6 pim interface	Displays detailed PIM settings for a specific interface.

MIB Objects

```
alaPimInterfaceAugTable
   alaPimBfdStatus
```

ipv6 pim bidir ssm-compat

Configures the status of the Source-specific Multicast (SSM) compatibility mode. When enabled, an IPv6 BIDIR-PIM router will support receiving MLDv2 SSM joins and process them as a (*,G) join.

ipv6 pim bidir ssm-compat {enable | disable}

Syntax Definitions

enable	Administratively enables the IPv6 BIDIR/SSM compatibility mode.
disable	Administratively disables IPv6 BIDIR/SSM compatibility mode.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the SSM compatibility mode is disabled, MLDv2 SSM joins are ignored by the IPv6 BIDIR-PIM router.
- This command is only applicable if IPv6 BIDIR-PIM is globally enabled for the switch.

Examples

```
-> ipv6 pim bidir ssm-compat enable
-> ipv6 pim bidir ssm-compat disable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6BidirSsmCompat
```

ipv6 pim bidir fast-join

Configures whether or not an IPv6 BIDIR-PIM router will automatically create (*,G) routes in the hardware as soon as IPv6 BIDIR (*,G) routes are learned.

ipv6 pim bidir fast-join {enable | disable}

Syntax Definitions

enable	Administratively enables the IPv6 BIDIR-PIM fast join functionality.
disable	Administratively disables the IPv6 BIDIR-PIM fast join functionality.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is only applicable if IPv6 BIDIR-PIM is globally enabled for the switch.
- When the IPv6 BIDIR fast join functionality is enabled, convergence of multicast traffic may occur faster because the (*,G) routes are already created before the actual multicast traffic is received.
- When the IPv6 BIDIR fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.

Examples

```
-> ipv6 pim bidir fast-join enable
-> ipv6 pim bidir fast-join disable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6BidirFastJoin
```

ipv6 pim sparse asm-fast-join

Configures whether or not an IPv6 PIM Sparse router will automatically create (*,G) routes in the hardware as soon as the IPv6 (*,G) routes are learned.

ipv6 pim sparse asm-fast-join {enable | disable}

Syntax Definitions

enable	Administratively enables the IPv6 PIM Sparse ASM fast join functionality.
disable	Administratively disables the IPv6 PIM Sparse ASM fast join functionality.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is only supported in the IPv6 PIM Sparse mode.
- When the IPv6 PIM Sparse fast join functionality is enabled, convergence of multicast traffic may occur faster because the (*,G) routes are already created before the actual multicast traffic is received.
- When the IPv6 PIM Sparse fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.
- This option should be used with caution due to the complicated nature of IPv6 PIM ASM, which involves forwarding on the shared tree, the sending and receiving of PIM register packets, and switching to the SPT. As a result, only enable the IPv6 ASM fast join function when there are no other locally attached sources, the router is not the RP, and the SPT is disabled.

Examples

```
-> ipv6 pim sparse asm-fast-join enable
-> ipv6 pim sparse asm-fast-join disable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6AsmFastJoin
```

ipv6 pim sparse ssm-fast-join

Configures whether or not an IPv6 PIM Sparse router will automatically create both IPv6 PIM Sparse and SSM (S,G) routes in the hardware as soon as the IPv6 (S,G) routes are learned.

ipv6 pim sparse ssm-fast-join {enable | disable}

Syntax Definitions

enable	Administratively enables the IPv6 PIM SSM fast join functionality.
disable	Administratively disables the IPv6 PIM SSM fast join functionality.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is only supported in the IPv6 PIM Sparse mode.
- When the IPv6 PIM Sparse fast join functionality is enabled, convergence of multicast traffic may occur faster because the (S,G) routes are already created before the actual multicast traffic is received.
- When the IPv6 PIM Sparse fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.

Examples

```
-> ipv6 pim sparse ssm-fast-join enable
-> ipv6 pim sparse ssm-fast-join disable
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
   alaPimsmV6SsmFastJoin
```

ipv6 pim joinprune-packing

Enable or disable PIM Join/Prune message packing.

ipv6 pim joinprune-packing {enable | disable}

Syntax Definitions

enable	Enable the PIM Join/Prune message packing.
disable	Disable the PIM Join/Prune message packing

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6860, 6900

Usage Guidelines

The value of disable can be used to disable this feature and return to the original operation of PIM where Join/Prune messages are not packed.

Examples

```
-> ipv6 pim joinprune-packing enable
-> ipv6 pim joinprune-packing disable
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimGlobalConfig
   alaPimV6JoinPruneMsgPackingStatus
```

show ipv6 pim sparse

Displays the status of the various global parameters for the IPv6 PIM sparse mode.

show ipv6 pim sparse

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim sparse
Status                     = disabled,
Keepalive Period           = 210,
Max RPs                    = 32,
Probe Time                 = 5,
Register Suppress Timeout  = 60,
RP Switchover              = enabled,
SPT Status                 = enabled,
BIDIR Status               = disabled,
BIDIR Periodic Interval    = 60,
BIDIR DF Abort Status      = disabled,
BFD Status                 = disabled,
ASM Fast Join              = disabled,
SSM Fast Join              = disabled,
BIDIR Fast Join            = disabled,
BIDIR SSM Compatibility    = disabled,
Register Rate Limit        = 100,
Join/Prune Message Packing = enabled
```

output definitions

Status	The current global (i.e., switch-wide) status of the IPv6 PIM sparse mode. Options include **enabled** and **disabled**.
Keepalive Period	The duration of the Keepalive timer. The default value is 210.
Max RPs	The maximum number of Rendezvous Points (RPs) allowed in the IPv6 PIM-SM domain (1–100). The default value is 32.

output definitions

Probe Time	The amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the RP. This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP. Values may range from 1 to 300. The default value is 5.
Register Suppress Timeout	The amount of time, in seconds, the DR will stop sending registers to the RP once a Register-Stop is received (1–300). The default value is 60.
RP switchover	The current status of the RP Switchover capability. RP switchover enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated data packet. Options include **enabled** and **disabled**. The default setting is **enabled**.
SPT Status	The current status of last hop DR switching to the SPT. Options include **enabled** and **disabled**. The default setting is **enabled**.
BIDIR Status	The current global status of Bidirectional PIM (BIDIR-PIM) for the switch. Options include **enabled** and **disabled** (the default).
BIDIR Periodic Interval	The amount of time, in seconds, between Winner messages the DF sends out to announce its status. The valid range is 0–2000. The default is 60 seconds.
BIDIR DF Abort Status	Indicates whether or not the Designated Forwarder (DF) election process is aborted when a PIM Hello message is received from a non-Bidirectional PIM (BIDIR-PIM) capable router. Options include **enabled** and **disabled** (the default).
BFD Status	Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is **enabled** or **disabled** (the default) for the PIM router.
ASM Fast Join	The status of the PIM Sparse fast join operation for ASM routes. When **enabled**, PIM ASM (*,G) routes are automatically created in hardware when the routes are initially learned; when **disabled** (the default), the (*,G) routes are not created in hardware until multicast traffic reaches the switch.
SSM Fast Join	The status of the PIM Sparse fast join operation for PIM Sparse and SSM routes. When **enabled**, PIM Sparse and SSM (S,G) routes are automatically created in hardware when the routes are initially learned; when **disabled** (the default), the (S,G) routes are not created in hardware until multicast traffic reaches the switch.
BIDIR Fast Join	The status of the BIDIR-PIM fast join operation. When **enabled**, BIDIR-PIM (*,G) routes are automatically created in hardware when the routes are initially learned; when **disabled** (the default), the (*,G) routes are not created in hardware until multicast traffic reaches the switch.
BIDIR SSM Compatibility	The status of the SSM compatibility mode. When **enabled**, a BIDIR-PIM router will accept and process SSM joins as (*,G) joins; when **disabled** (the default), SSM joins are ignored.
Register Rate Limit	The per (S,G) register rate limit in packets per second.
Join/Prune Message Packing	The current status of PIM Join/Prune message packing. Options include **enabled** and **disabled**.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; BIDIR fields added.
Release 8.3.1.R02; **ASM Fast Join**, **SSM Fast Join**, **BIDIR Fast Join**, and **BIDIR SSM Compatibility** fields added.
Release 8.4.1.R02; **Register Rate Limit** field added.
Release 8.6R1; **Join/Prune Message Packing** field added.

Related Commands

ipv6 pim sparse admin-state	Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.
ip pim keepalive-period	Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
ip pim max-rps	Configures the maximum number of C-RP routers allowed in the PIM-SM domain.
ip pim probe-time	Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.
ip pim register-suppress-timeout	Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.
ipv6 pim rp-switchover	Enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated packet in the IPv6 PIM domain.
ipv6 pim register-rate-limit	Specifies the maximum number of PIM Register Packets that the Designated Router (DR) will send per second for each (S,G) entry.
ipv6 pim spt admin-state	Enables or disables last hop DR switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first multicast data packet is received.
ipv6 pim bidir admin-state	Globally enables or disables BIDIR-PIM protocol on the switch.
ip pim df-periodic-interval	Configures the time interval at which the DF for each RP address periodically announces its status in a Winner message
ip pim df-abort	Configures whether or not the DF election process is stopped when a PIM Hello message received from a PIM neighbor does not contain the Bidirectional Capable option.
ipv6 pim interface	Enables IPv6 PIM and configures statistics on the interface.
ipv6 pim bfd-state	Enables or disables BFD for the PIM router.
ipv6 pim sparse asm-fast-join	Configures the status of the PIM Sparse fast join operation for ASM routes.
ipv6 pim sparse ssm-fast-join	Configures the status of the PIM Sparse fast join operation for both PIM Sparse and SSM routes.
ipv6 pim bidir fast-join	Configures the status of the BIDIR-PIM fast join operation.

ipv6 pim bidir ssm-compat	Configures the SSM compatibility mode for a BIDIR-PIM router.
ipv6 pim joinprune-packing	Enable or disable PIM Join/Prune message packing.

MIB Objects

```
ALCATEL-IND1-PIM-MIB.mib
alaPimsmGlobalConfig
   alaPimsmV6AdminStatus
   alaPimsmMaxRPS
   alaPimsmProbeTime
   alaPimsmV6RPSwitchover
   alaPimsmV6AdminSPTConfig
   alaPimsmBidirStatus
   alaPimsmBidirPeriodicInterval
   alaPimsmBidirDFAbort
   alaPimsmV6AsmFastJoin
   alaPimsmV6SsmFastJoin
   alaPimsmV6BidirFastJoin
   alaPimsmV6BidirSsmCompat
alaPimGlobalConfig
   alaPimV6BfdStatus
   alaPimV6JoinPruneMsgPackingStatus
PIM-STD-MIB.mib
pim
   pimKeepalivePeriod
   pimRegisterSuppressionTime
```

show ipv6 pim dense

Displays the status of the various global parameters for the IPv6 PIM dense mode.

show ipv6 pim dense

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim dense
Status                       = enabled,
Source Lifetime              = 210,
State Refresh Interval       = 60,
State Refresh Limit Interval = 0,
State Refresh TTL            = 16
BFD Status                   = enabled
```

output definitions

Status	The current global (i.e., switch-wide) status of the IPv6 PIM dense mode. Options include **enabled** and **disabled**.
Source Lifetime	The duration of the Keepalive or Source Lifetime timer. The default value is 210.
State Refresh Interval	The time-interval, in seconds, between successive State Refresh messages originated by the router. The default value is 60.
State Refresh Limit Interval	Displays the limit at which a router will not forward the State Refresh messages, if they are received at less than the interval. The default value is 0.
State Refresh TTL	Displays the TTL to be used in the router's originated State Refresh messages. The default value is 16.
BFD Status	Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is **enabled** or **disabled** (the default) for PIM router.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim dense admin-state	Enables or disables IPv6 PIM-DM (dense mode) globally on the switch.
ip pim keepalive-period	Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
ip pim state-refresh-interval	Sets the interval between successive State Refresh messages originated by a router.
ip pim state-refresh-limit	Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.
ip pim state-refresh-ttl	Sets the Time to Live to be used in a router's originated State Refresh messages if the data packet's Time to Live is not recorded.
ipv6 pim bfd-state	Enables or disables BFD for the PIM router.

MIB Objects

```
ALCATEL-IND1-PIM-MIB.mib
alaPimdmGlobalConfig
   alaPimdmV6AdminStatus
   alaPimRefreshInterval
   alaPimdmStateRefreshLimitInterval
   alaPimdmStateRefreshTimeToLive
alaPimGlobalConfig
   alaPimV6BfdStatus
PIM-STD-MIB.mib
pim
   pimKeepalivePeriod
```

show ipv6 pim ssm group

Displays the static configuration of IPv6 multicast group mappings for PIM-Source Specific Multicast (SSM).

show ipv6 pim ssm group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim ssm group

Group Address/Prefix RP Address      Mode  Override Precedence Status
--------------------+---------------+-----+--------+----------+-------
ff00::/8             ::              ssm   false    none       enabled
ff34::/32            ::              ssm   false    none       enabled
```

output definitions

Group Address/Prefix	The IPv6 multicast group address along with the prefix length.
RP Address	The IPv6 address of the Rendezvous Point (RP) for groups within this group prefix
Mode	The IPv6 PIM mode that is used for the groups in this prefix.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that can be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim ssm group	Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

MIB Objects

```
pimStaticRPTable
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPRPAddress
   pimStaticRPPimMode
   pimStaticRPOverrideDynamic
   pimStaticRPPrecedence
   pimStaticRPRowStatus
```

show ipv6 pim dense group

Displays the static configuration of IPv6 multicast group mappings for PIM Dense Mode (DM).

show ipv6 pim dense group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim dense group
Group Address/Prefix RP Address      Mode  Override Precedence Status
--------------------+---------------+-----+--------+----------+-------
ff00::/8             ::              dm    false    none       enabled
ff34::/32            ::              dm    false    none       enabled
```

output definitions

Group Address/Pref	The IPv6 multicast group address along with the prefix length.
RP Address	The IPv6 address of the Rendezvous Point (RP) for groups within this group prefix
Mode	The IPv6 PIM mode that is used for the groups in this prefix.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that can be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim dense group	Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

MIB Objects

```
alaPimdmDenseGroupTable
   alaPimdmDenseGroupGrpAddress
   alaPimdmDenseGroupGrpPrefixLength
   alaPimdmDenseGroupOverrideDynamic
   alaPimdmDenseGroupPrecedence
   alaPimdmDenseGroupRowStatus
```

show ipv6 pim interface

Displays detailed IPv6 PIM settings for a specific interface. In general, it displays IPv6 PIM settings for all the interfaces if no argument is specified.

show ipv6 pim interface [*if_name***]**

Syntax Definitions

if_name	The name of the interface.

Defaults

By default, a summary list of all IPv6 PIM interfaces is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

To view more detailed information about a particular interface, specify the interface name in the command line. Additional information includes Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

Examples

```
-> show ipv6 pim interface

Total 0 Interfaces

Interface Name      Designated                  Hello    J/P      Oper     BFD
                    Router                      Interval Interval Status   Status
--------------------+---------------------------+--------+--------+--------+--------
vlan-5              fe80::2d0:95ff:feac:a537    30       60       enabled  disabled
vlan-30             fe80::2d0:95ff:feac:a537    30       60       disabled disabled
vlan-40             fe80::2d0:95ff:fee2:6eec    30       60       enabled  disabled

-> show ipv6 pim interface vlan-5
Interface Name              = vlan-5,
IP Address                  = fe80::2d0:95ff:fee2:6eec,
Designated Router           = fe80::2d0:95ff:fee2:a537,
Hello Interval              = 30,
Triggered Hello Interval    = 5,
Hello HoldTime              = 105,
Join/Prune Interval         = 60,
Join/Prune HoldTime         = 210,
Propagation (Prune) Delay   = 500,
Override Interval           = 2500,
Generation ID               = 0x4717be4d,
DR Priority                 = 1,
DR Priority Enabled         = true,
Lan Delay Enabled           = true,
Effective Propagation Delay = 500,
```

```
Effective Override Interval = 2500,
Suppression Enabled         = true,
Stub Interface              = false,
Prune Limit Interval        = 60,
Graft Retry Interval        = 3,
State Refresh Enabled       = true,
BiDir Capable               = false,
DF Election Robustness      = 3,
Operational Status          = enabled,
BFD Status                  = disabled,
Join/Prune MTU              = 1000,
Join/Prune Triggered Delay  = 100
```

output definitions

Interface Name	The name of the IPv6 PIM interface.
IPv6 address	Specifies the IPv6 address of the specified interface.
Designated Router	The primary IP address for the Designated Router (DR). The DR acts on behalf of any directly-connected hosts with respect to the PIM-SM protocol. Only one router in the LAN will act as the DR.
Hello Interval	The frequency at which PIM Hello messages are transmitted on a specified interface. Values may range from 1 to 18000. The default value is 30.
Join/Prune Interval	The Join/Prune interval for the associated interface. The Join/Prune interval is the interval at which periodic PIM-SM Join/Prune messages are sent. Values may range from 0 to 18000. The default value is 60.
Triggered Hello Interval	The current Triggered Hello Interval. This value indicates the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface. Values may range from 0 to 60. The default value is 5.
Hello Holdtime	The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 105.
Join/Prune Holdtime	The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 210.
Propagation Delay	The expected propagation delay between PIM routers on the network. Values may range from 0 to 32767. The default value is 500.
Override Interval	The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.
Generation ID Option	The value of the Generation ID this router inserted in the last PIM Hello message it sent on this interface.

output definitions (continued)

DR Priority	Displays the Designated Router priority for each interface. This value is used in determining the Designated Router on an interface. Values may range from 1 to 192. A higher numeric value denotes a higher priority. Note that priority-based election is used only if all routers on the interface are using the DR priority option. The default value is 1.
Lan Delay Enabled	Options include **true** and **false**. The value will be true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting will be false.
Effective Propagation Delay	The Effective Propagation Delay on this interface.
Effective Override Interval	The Effective Override Interval on this interface.
Suppression Enabled	Specifies whether the Join suppression is enabled on this interface.
DR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the DR Priority option.
Stub Interface	Specifies whether this interface is a 'stub interface'. If this is TRUE, then no PIM packets are sent out on this interface, and any received PIM packets are ignored.
Prune Limit Interval	The minimum interval that must transpire between two successive Prunes sent by a router. This is used only with PIM-DM. Values may range from 0 to 65535. The default value is 60.
Graft Retry Interval	Displays the time-interval a router waits for a Graft acknowledgment before resending a Graft on the interface. This is only used with PIM-DM. Values may range from 0 to 65535. The default value is 3.
SR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the State Refresh option. This is used only by PIM-DM.
BiDir Capable	Evaluates to TRUE if all routers on this interface are using the Bidirectional Capable option. This is used only by BIDIR-PIM.
DF Election Robustness	The minimum number of PIM Designated Forwarder (DF) Election messages that must be lost to determine that the DF Election process has failed for this interface. This is used only by BIDIR-PIM.
Operational Status	The current operational status of the corresponding interface. Options include **enabled** and **disabled**. This value indicates whether the IPv6 interface is operationally up. For example, if PIM is enabled on the interface, but the interface is currently down, this field will display as disabled. The default setting is **disabled**. To enable or disable PIM on an interface, refer to the **ipv6 pim interface** command on page 33-124. To globally enable or disable PIM on the switch, refer to the **ipv6 pim sparse admin-state** command on page 33-106 and **ipv6 pim dense admin-state** command on page 33-108.
BFD Status	Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is **enabled** or **disabled** (the default) for the PIM interface. Configured through the **ipv6 pim interface bfd-state** command.
Join/Prune MTU	The configured PIM Join/Prune packet MTU for this interface.
Join/Prune Triggered Delay	The triggered Join/Prune delay.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **BiDir Capable** and **DF Election Robustness** fields added.
Release 8.6R1; **Join/Prune MTU** and **Join/Prune Triggered** Delay fields added.

Related Commands

ipv6 pim interface	Enables IPv6 PIM and configures statistics on the interface.

MIB Objects

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceIPVersion
   pimInterfaceAddressType
   pimInterfaceAddress
   pimInterfaceGenerationIDValue
   pimInterfaceDR
   pimInterfaceDRPriority
   pimInterfaceDRPriorityEnabled
   pimInterfaceHelloInterval
   pimInterfaceTrigHelloInterval
   pimInterfaceHelloHoldtime
   pimInterfaceJoinPruneInterval
   pimInterfaceJoinPruneHoldtime
   pimInterfaceDFElectionRobustness
   pimInterfaceLanDelayEnabled
   pimInterfacePropagationDelay
   pimInterfaceOverrideInterval
   pimInterfaceEffectPropagDelay
   pimInterfaceEffectOverrideIvl
   pimInterfaceSuppressionEnabled
   pimInterfaceBidirCapable
   pimInterfaceDomainBorder
   pimInterfaceStubInterface
   pimInterfacePruneLimitInterval
   pimInterfaceGraftRetryInterval
   pimInterfaceSRPriorityEnabled
   pimInterfaceStatus
alaPimInterfaceAugTable
   alaPimInterfaceBfdStatus
   alaPimInterfaceJoinPruneMtu
   alaPimInterfaceJoinPruneDelay
```

show ipv6 pim neighbor

Displays a list of active IPv6 PIM neighbors.

show ipv6 pim neighbor [*ipv6_address***] [***if_name***]**

Syntax Definitions

ipv6_address	The IPv6 address for the PIM neighbor.
if_name	The name of the interface.

Defaults

If the neighbor's IPv6 address or interface name is not specified, the entire IPv6 PIM neighbor table is displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

To view more detailed information about a particular neighbor, specify the neighbor's IPv6 address or the associated interface name in the command line. Additional information will be displayed, which includes LAN Prune Delay, Override Interval, TBit field, State Refresh capable, and Designated Router option status.

Examples

```
-> show ipv6 pim neighbor
Neighbor Address               Interface Name       Uptime      Expires     DR Pri
------------------------------+--------------------+-----------+-----------+------
fe80::2d0:95ff:feac:a537       vlan-30               02h:56m:51s 00h:01m:28s 1
```

If a specific neighbor address is specified in the command line, *detailed information for the corresponding neighbor only* displays:

```
-> show ipv6 pim neighbor fe80::2d0:95ff:feac:a537
vlan-30
  Neighbor IPv6 Address        = fe80::2d0:95ff:feac:a537,
  Uptime                       = 02h:57m:09s,
  Expires                      = 00h:01m:40s,
  Lan Prune Delay Present      = True,
  Propagation Delay            = 500,
  Override Interval            = 2500,
  TBit Field                   = True,
  Gen ID Present               = True,
  Gen ID Value                 = 0x7720c123,
  BiDir Capable                = False,
  DR Priority Present          = True,
  DR Priority                  = 1,
  State Refresh Capable        = True,
  Secondary Addresses:
    3000::11
```

```
vlan-40
  Neighbor IPv6 Address        = fe80::2d0:95ff:feac:a537,
  Uptime                       = 03h:57m:03s,
  Expires                      = 00h:01m:20s,
  Lan Prune Delay Present            = True,
  Propagation Delay            = 500,
  Override Interval            = 2500,
  TBit Field                   = True,
  Gen ID Present               = True,
  Gen ID Value                 = 0x7720c123,
  BiDir Capable                = False,
  DR Priority Present          = True,
  DR Priority                  = 1,
  State Refresh Capable        = True,
  Secondary Addresses:
    4000::11
```

If a specific interface name is specified in the command line, *detailed information corresponding to all neighbors on the specified interface only* displays:

```
-> show IPv6 pim neighbor vlan-30
vlan-30
  Neighbor IPv6 Address        = fe80::2d0:95ff:feac:a537,
  Uptime                       = 02h:57m:09s,
  Expires                      = 00h:01m:40s,
  Lan Prune Delay Present            = True,
  Propagation Delay            = 500,
  Override Interval            = 2500,
  TBit Field                   = True,
  Gen ID Present               = True,
  Gen ID Value                 = 0x7720c123,
  BiDir Capable                = False,
  DR Priority Present          = True,
  DR Priority                  = 1,
  State Refresh Capable        = True,
  Secondary Addresses:
    3000::11
```

output definitions

Neighbor IPv6 Address	The IPv6 address of the active PIM neighbor.
Interface Name	The name of the IPv6 PIM interface that is used to reach the neighbor.
Uptime	The amount of time since this PIM neighbor last became a neighbor of the local router, displayed in hours, minutes, and seconds.
Expires	The minimum amount of time remaining before the PIM neighbor will be aged out, displayed in hours, minutes, and seconds.
LAN Prune Delay present	Specifies whether this neighbor is using the LAN Prune Delay option. Options include **true** or **false**.
Propagation Delay	The value of the propagation-delay field of the LAN prune-delay option received from this neighbor. A value of 0 indicates that no LAN prune-delay option was received from this neighbor.

output definitions (continued)

Override Interval	The current Override Interval of the LAN prune-delay option received from this neighbor. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by the neighboring router is dictated by this number. Values may range from 0 to 65535. A value of 0 indicates that no LAN prune-delay option was received from this neighbor.
TBit field	The value of the Tbit field of the LAN prune-delay option received from this neighbor. The Tbit specifies the ability of the neighbor to disable Join suppression.
Gen ID present	Specifies whether this neighbor is using Generation ID option. Options include **true** or **false**.
Gen ID Value	The value of the Generation ID in the last PIM Hello message received from this neighbor.
BiDir Capable	Specifies whether this neighbor is using the Bidirectional-PIM Capable option.
DR Priority Present	Displays whether the neighbor is using the Designated Router option. Options include **true** or **false**.
DR priority	The value of the Designated Router Priority in the last PIM Hello message received from this neighbor.
State Refresh Capable	Displays whether the neighbor is capable of receiving State Refresh messages. Options include **true** or **false**.
Secondary Addresses	The secondary IPv6 address of this PIM neighbor.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
pimNeighborTable
   pimNeighborIfIndex
   pimNeighborAddressType
   pimNeighborAddress
   pimNeighborGenerationIDPresent
   pimNeighborGenerationIDValue
   pimNeighborUpTime
   pimNeighborExpiryTime
   pimNeighborDRPriorityPresent
   pimNeighborDRPriority
   pimNeighborLanPruneDelayPresent
   pimNeighborTBit
   pimNeighborPropagationDelay
   pimNeighborOverrideInterval
   pimNeighborBidirCapable
```

```
   pimNeighborSRCapable
pimNbrSecAddressTable
   pimNbrSecAddressIfIndex
   pimNbrSecAddressType
   pimNbrSecAddressPrimary
   pimNbrSecAddress
```

show ipv6 pim static-rp

Displays the IPv6 PIM Static RP table, which includes IPv6 multicast group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the static RP configuration (i.e., enabled or disabled).

show ipv6 pim static-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim static-rp

Group Address/Pref Length   RP Address    Mode  Override Precedence Status
----------------------------+-------------+-----+--------+----------+--------
ff00::/8                    3000::11      asm   false    none       enabled
ff08::/32                   2100::8       bidir false    none       enabled
```

output definitions

Group Address/Pref Length	The IPv6 multicast group address along with the prefix length.
RP Address	The IPv6 address of the RP that is mapped for the groups within the group prefix. This field is set to zero, if the specified IPv6 PIM mode is SSM or DM.
Mode	The PIM mode to be used for groups in this prefix. The possible values include **asm**, **ssm**, **dm**, or **bidir**.
Override	Specifies that this static RP configuration can override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that is used for this static RP configuration.
Status	Displays whether the static RP configuration is currently enabled or disabled. Options include **enabled** and **disabled**.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **bidir** mode support added.

Related Commands

ipv6 pim static-rp	Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

MIB Objects

```
pimStaticRPTable
   pimStaticRPAddressType
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPRPAddress
   pimStaticRPPimMode
   pimStaticRPOverrideDynamic
   pimStaticRPPrecedence
   pimStaticRPRowStatus
   pimStaticRPStorageType
```

show ipv6 pim anycast-rp

Displays the anycast RP table, which includes the anycast RP address, the RP address, if its the local router, and the current status of the anycast RP configuration.

show ipv6 pim anycast-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim anycast-rp
Anycast RP Address      Router Address      Local    Status
--------------------+------------------+---------+---------
2001:1::1               3001:1::1         true     enabled
2001:1::1               3001:1::2         false    enabled
```

output definitions

Anycast RP Address	The anycast RP address.
Router Address	The router IPv6 address that is a member of the anycast RP set.
Local	Displays whether this entry corresponds to the local router. The value will display true if this entry corresponds to the local router and false if it does not correspond to the local router.
Status	Displays whether the anycast RP configuration is currently enabled or disabled. To change the current status, refer to the ipv6 pim anycast-rp command.

Release History

Release 8.6R2; command introduced.

Related Commands

ipv6 pim anycast-rp	Configures the anycast RP set, which is the set of all routers that would act as the RP.

MIB Objects

```
pimAnycastRPSetTable
   pimAnycastRPSetAddressType
   pimAnycastRPSetAnycastAddress
   pimAnycastRPSetRouterAddress
   pimAnycastRPSetLocalRouter
   pimAnycastRPSetRowStatus
```

show ipv6 pim group-map

Displays the IPv6 PIM group mapping table.

show ipv6 pim group-map [bsr | static-rp | ssm | dense]

Syntax Definitions

N/A

Defaults

If the keywords **bsr**, **static-rp**, **ssm**, or **dense** are included in the command line, then only the entries that were created by the specified origin are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined through the **ipv6 pim static-rp** command. As long as the RP addresses defined in the static RP set are reachable, they will be added to the group mapping table.
- If the IPv6 multicast groups are mapped to the mode DM or SSM, then the entries created by local SSM address range configuration using the **ipv6 pim ssm group** command and local Dense Mode address range configuration using the **ipv6 pim dense group** command are displayed.
- If the bootstrap mechanism is being used, this information is obtained from received Candidate-RP advertisements (when the local router is the BSR; when the local router is not the BSR, this information is obtained from received bootstrap messages).

Examples

```
-> show ipv6 pim group-map
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+------------+-----+-----------
BSR       ff00::/8                   2000::8       bidir 192
BSR       ff00::/8                   3000::11      asm   192
BSR       ff00::/8                   4000::7       asm   192
SSM       ff33::/32                                ssm

-> show ipv6 pim group-map bsr
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+------------+-----+-----------
BSR       ff00::/8                   2000::8       bidir 192
BSR       ff00::/8                   3000::11      asm   192
BSR       ff00::/8                   4000::7       asm   192

-> show ipv6 pim group-map ssm
Origin     Group Address/Pref Length   RP Address    Mode  Precedence
---------+--------------------------+------------+-----+-----------
SSM       ff33::/32                                ssm
```

output definitions

Origin	The mechanism by which the PIM mode and RP for the group were learned. The possible values include 'static RP' for local static RP configuration, 'static SSM' for both static SSM group configuration and Dense Mode Group configuration, and 'BSR' for the PIM Bootstrap Router mechanism.
Group Address/Prefix Length	The IPv6 multicast group address along with the prefix length.
RP Address	The IPv6 address of the Rendezvous Point to be used for groups within the group prefix.
Mode	The IPv6 PIM mode to be used for groups in this prefix. The possible values include **asm**, **ssm**, **dm**, or **bidir**.
Mapping Precedence	The precedence value of a particular row, that determines which row applies to a given group address. Numerically higher values for this object indicate lower precedences, with the value zero denoting the highest precedence.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **bidir** mode support added.

Related Commands

ipv6 pim static-rp	Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).
ipv6 pim ssm group	Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).
ipv6 pim dense group	Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

MIB Objects

```
pimGroupMappingTable
   pimGroupMappingOrigin
   pimGroupMappingAddressType
   pimGroupMappingGrpAddress
   pimGroupMappingGrpPrefixLength
   pimGroupMappingRPAddressType
   pimGroupMappingRPAddress
   pimGroupMappingPimMode
   pimGroupMappingPrecedence
```

show ipv6 pim candidate-rp

Displays the IPv6 multicast groups for which the local router advertises itself as a Candidate-RP.

show ipv6 pim candidate-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim candidate-rp
RP Address       Group Address       Priority  Interval  Mode  Status
----------------+-------------------+---------+---------+-----+---------
2000::8          ff00::/8            192       60        bidir enabled
```

output definitions

RP Address	An IPv6 unicast address that is advertised as the Candidate-Rendezvous Point (RP).
Group Address	The IPv6 multicast group address along with the prefix length. This is the group for which the local router advertises itself as a C-RP.
Priority	The C-RP router's priority. The lower the value, the higher the priority.
Interval	The time interval at which the C-RP advertisements are sent to the BSR.
Mode	Whether or not the Group Address is for a PIM-SM group or a Bidirectional PIM (BIDIR-PIM) group.
Status	The current status of this entry. The status is shown as enabled only if the IPv6 PIM-SM is globally enabled and the IPv6 PIM interface is enabled.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **Mode** field added.

Related Commands

ipv6 pim candidate-rp	Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IPv6 multicast group(s).

MIB Objects

```
pimBsrCandidateRPTable
   pimBsrCandidateRPAddressType
   pimBsrCandidateRPAddress
   pimBsrCandidateRPGroupAddress
   pimBsrCandidateRPGroupPrefixLength
   pimBsrCandidateRPBidir
   pimBsrCandidateRPAdvTimer
   pimBsrCandidateRPPriority
   pimBsrCandidateRPAdvInterval
   pimBsrCandidateRPHoldtime
   pimBsrCandidateRPStatus
   pimBsrCandidateRPStorageType
```

show ipv6 pim cbsr

Displays the IPv6 Candidate-BSR information that is used in the Bootstrap messages.

show ipv6 pim cbsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim cbsr
CBSR Address             = 3000::7,
Status                   = enabled,
CBSR Priority            = 0,
Hash Mask Length         = 126,
Elected BSR              = False,
Timer                    = 00h:00m:00s
```

output definitions

CBSR Address	An IPv6 unicast address that the local router uses to advertise itself as a Candidate-BSR.
Status	The current status of this entry. The status is shown as enabled only if the IPv6 PIM-SM is globally enabled and the IPv6 PIM interface is enabled.
CBSR Priority	The value for the local router as a Candidate-BSR. The higher the value, the higher the priority.
Hash Mask Length	The hash mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for an IPv6 multicast group)
Elected BSR	Specifies whether the local router is the elected BSR.
Timer	The time value that is remaining before the local router originates the next Bootstrap message. This value is zero if this router is not the elected BSR.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim cbsr	Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBSrCandidateBSRTable
   pimBsrCandidateBSRZoneIndex
   pimBsrCandidateBSRAddressType
   pimBsrCandidateBSRAddress
   pimBsrCandidateBSRPriority
   pimBsrCandidateBSRHashMaskLength
   pimBsrCandidateBSRElectedBSR
   pimBsrCandidateBSRBootstrapTimer
   pimBsrCandidateBSRStatus
```

show ipv6 pim bsr

Displays information about the elected IPv6 BSR.

show ipv6 pim bsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim bsr
BSR Address              = 3000::7,
BSR Priority             = 192,
Hash Mask Length         = 126,
Expiry Time              = 00h:01m:35s
```

output definitions

BSR Address	The IPv6 unicast address of the elected BSR.
BSR Priority	The priority value of the elected BSR. The higher the value, the higher the priority.
Hash Mask Length	The hash mask length that is advertised in the Bootstrap messages by the elected BSR (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group.
Expiry Time	The minimum time remaining before the elected BSR will be declared down.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim cbsr	Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
pimBsrElectedBSRTable
   pimBsrElectedBSRZoneIndex
   pimBsrElectedBSRAddressType
   pimBsrElectedBSRAddress
   pimBsrElectedBSRPriority
   pimBsrElectedBSRHashMaskLength
   pimBsrElectedBSRExpiryTime
```

show ipv6 pim groute

Displays (*,G) routing table entries for IPv6 PIM.

show ipv6 pim groute [*group_address***]**

Syntax Definitions

group_address	The IPv6 address of the Multicast Group.

Defaults

By default, entire (*,G) routing table is displayed. To view more detailed (*,G) state information about a particular group, specify the group address in the command line.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

When the *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.

Examples

```
-> show ipv6 pim groute
Total 1 (*,G)

Group Address        RP Address        RPF Interface           UpTime       Mode
--------------------+-----------------+-----------------------+------------+-------
ff08::2              2000::8           vlan-200                00h:05m:42s  bidir
ff0e::7              5ffe::3           vlan-4                  00h:01m:23s  asm

-> show ipv6 pim groute ff0e::7
(*,ff0e::7)
  UpTime                  = 00h:01m:28s
  RP Address              = 5ffe::3,
  PIM Mode                = ASM,
  PIM Mode Origin         = BSR,
  Upstream Join State     = Not Joined,
  Upstream Join Timer     = 00h:00m:00s,
  Upstream Neighbor       = fe80::220:fcff:fe1e:2455,
  RPF Interface           = vlan-4,
  RPF Next Hop            = fe80::220:fcff:fe1e:2455,
  RPF Route Protocol      = Static,
  RPF Route Address       = 5ffe::3/128,
  RPF Route Metric Pref   = 10,
  RPF Route Metric        = 10,
  Interface Specific State:
    vlan-3
      UpTime                    = 00h:01m:28s,
      Local Membership          = False,
      Join/Prune State          = Joined,
```

```
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:02m:02s,
    Assert State              = Loser,
    Assert Timer              = 00h:01m:32s,
    Assert Winner Address     = fe80::220:fcff:fe1e:2454,
    Assert Winner Metric Pref = 9 (rpt),
    Assert Winner Metric      = 10,
  vlan-4
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-5
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
```

output definitions

Group-address	The IPv6 Multicast Group Address.
RP Address	The address of the Rendezvous Point (RP) for the group.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
UpTime	The time since this entry was created.
Mode	Whether this entry represents an **asm**, (Any Source Multicast) or **bidir** (Bidirectional PIM) group.
Pim Mode Origin	The mechanism by which the PIM mode and RP for the group were learned.
Upstream Join State	Whether the local router should join the RP tree for the group.
Upstream Join Timer	The time remaining before the local router next sends a periodic (*,G) Join message on the RPF IfIndex.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (*,G) join messages to.
RPF Next Hop	The address of the RPF next hop towards the RP.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF interface towards the RP was learned.
RPF Route Address/Prefix Length	The IPv6 address combined with the prefix length identifies the route used to find the RPF interface towards the RP.
Route Metric Pref	The metric preference of the route used to find the RPF interface towards the RP.
Route Metric	The routing metric of the route used to find the RPF interface towards the RP.
Interface Name	The interface name that corresponds to the ifIndex.

output definitions (continued)

Local Membership	Whether the local router has (*,G) local membership on this interface.
Join Prune State	The state resulting from (*,G) Join/Prune messages received on this interface.
Prune Pending Timer	The time remaining before the local router acts on a (*,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.
Join Expiry Timer	The time remaining before (*,G) Join state for this interface expires.
Assert State	The (*,G) Assert state for this interface. The possible values are No Info, Winner or Loser.
Assert Timer	If Assert State is 'Winner', this is the time remaining before the local router next sends a (*,G) Assert message on this interface. If the Assert State is 'Loser', this is the time remaining before the (*,G) assert state expires.
Assert Winner Address	If the Assert State is 'Loser', this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is 'Loser', this is the metric preference of the route to the RP advertised by the assert winner; otherwise, this is zero.
Assert Winner Metric	If the Assert State is 'Loser', this is the routing metric of the route to the RP advertised by the assert winner; otherwise, this is zero.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; Mode field added, **bidir** mode support added

Related Commands

show ipv6 pim sgroute	Displays (S,G) state routing table entries.

MIB Objects

pimStarGTable

- pimStarGAddressType
- pimStarGGrpAddress
- pimStarGUpTime
- pimStarGPimMode
- pimStarGRPAddressType
- pimStarGRPAddress
- pimStarGPimModeOrigin
- pimStarGRPIsLocal
- pimStarGUpstreamJoinState
- pimStarGUpstreamJoinTimer
- pimStarGUpstreamNeighborType
- pimStarGUpstreamNeighbor
- pimStarGRPFIfIndex
- pimStarGRPFNextHopType
- pimStarGRPFNextHop
- pimStarGRPFRouteProtocol
- pimStarGRPFRouteAddress
- pimStarGRPFRoutePrefixLength
- pimStarGRPFRouteMetricPref
- pimStarGRPFRouteMetric

pimStarGITable

- pimStarGIIfIndex
- pimStarGIUpTime
- pimStarGILocalMembership
- pimStarGIJoinPruneState
- pimStarGIPrunePendingTimer
- pimStarGIJoinExpiryTimer
- pimStarGIAssertState
- pimStarGIAssertTimer
- pimStarGIAssertWinnerAddressType
- pimStarGIAssertWinnerAddress
- pimStarGIAssertWinnerMetricPref
- pimStarGIAssertWinnerMetric

show ipv6 pim sgroute

Displays (S,G) routing table entries for IPv6 PIM.

show ipv6 pim sgroute [*source_address group_address***]**

Syntax Definitions

source_address	The IPv6 address for a specific multicast source.
group_address	A IPv6 multicast address.

Defaults

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the *source_address* and *group_address* associated with that entry.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the *source_address* and *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IPv6 address is not specified, the current PIM status for all multicast route entries are displayed.

Examples

```
-> show ipv6 pim sgroute

Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
               L = Local, R = RPT, T = SPT, F = Register,
               P = Pruned, O = Originator

Total 1 (S,G)

Source Address        Group Address         RPF Interface    UpTime      Flags
---------------------+---------------------+----------------+-----------+------
8ffe::3               ff0e::7                                00h:01m:34s  SR


-> show ipv6 pim sgroute 8ffe::3 ff0e::7
(8ffe::3,ff0e::7)
  UpTime                  = 00h:01m:40s
  PIM Mode                = ASM,
  Upstream Join State     = Not Joined,
  Upstream RPT State      = Not Pruned,
  Upstream Join Timer     = 00h:00m:00s,
  Upstream Neighbor       = none,
  SPT Bit                 = False,
  DR Register State       = No Info,
  DR Register Stop Timer  = 00h:00m:00s,
  Interface Specific State:
```

```
vlan-3
  UpTime                    = 00h:01m:40s,
  Local Membership          = False,
  Join/Prune State          = No Info,
  RPT State                 = No Info,
  Prune Pending Timer       = 00h:00m:00s,
  Join Expiry Timer         = 00h:00m:00s,
  Assert State              = No Info,
  Assert Timer              = 00h:00m:00s,
vlan-4
  UpTime                    = 00h:00m:00s,
  Local Membership          = False,
  Join/Prune State          = No Info,
  RPT State                 = No Info,
  Prune Pending Timer       = 00h:00m:00s,
  Join Expiry Timer         = 00h:00m:00s,
  Assert State              = No Info,
  Assert Timer              = 00h:00m:00s,
vlan-5
  UpTime                    = 00h:00m:00s,
  Local Membership          = False,
  Join/Prune State          = No Info,
  RPT State                 = No Info,
  Prune Pending Timer       = 00h:00m:00s,
  Join Expiry Timer         = 00h:00m:00s,
  Assert State              = No Info,
  Assert Timer              = 00h:00m:00s,
```

output definitions

Source-address	The IPv6 Source address.
Group-address	The IPv6 Multicast Group Address.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (S,G) join messages to.
UpTime	The time since this entry was created.
Flags	Flags indicating SPTBit, Prune State, Join State, etc.
Pim Mode	Whether the Group Address is SSM, ASM or DM.
Upstream Join State	Whether the local router should join the SPT for the source and group represented by this entry.
Upstream Join Timer	The time remaining before the local router next sends a periodic (S,G) Join message.
RPF Next Hop	The address of the RPF next hop towards the source.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF Interface towards the source was learned.
RPF Route Address/Prefix Length	The IP address which when combined with the Route Prefix length identifies the route used to find the RPF interface towards the source.
RPF Route Metric Pref	The metric preference of the route used to find the RPF interface towards the source.

output definitions (continued)

RPF Route Metric	The metric preference of the route used to find the RPF interface towards the source.
DR Register State	Whether the local router should encapsulate (S,G) data packets in Register messages and send them to the RP. The possible values include No Info, Join, Join Pending, or Prune.
DR Register Stop Timer	The value of the Register Stop Timer. If the Register State is 'prune', this is the time remaining before the local router sends a Null-Register message to the RP. If the State is 'joinPending', this is the time remaining before the local router resumes encapsulating data packets and sending them to the RP.
Upstream Prune State	Whether the local router has pruned itself from the tree. This is only used by PIM-DM. The possible values include forwarding, Ack Pending, or Pruned.
Upstream Prune Limit Timer	The time remaining before the local router may send a (S,G) prune message on alaPimSGRPFIfIndex. This is only used by PIM-DM.
Originator State	Whether this router is an originator for the (S,G) message flow. This is only used by PIM-DM. The possible values include Not Originator or Originator.
Source Active Timer	If this router is the Originator, this is the time remaining before the local router reverts to notOriginator state. Otherwise, this is zero. This is only used by PIM-DM.
State Refresh Timer	If Originator state is 'originator', this is the time remaining before the local router sends a State Refresh Message. Otherwise, this is zero. This is only used by PIM-DM.
Interface Name	The interface name corresponding to the ifIndex that corresponds to this entry.
Uptime	The time since this entry was created.
Local Membership	Whether the local router has (S,G) local membership on this interface.
Join Prune State	The state resulting from (S,G) Join/Prune messages received on this interface. The possible values include No Info, Join, or Prune Pending.
Prune Pending Timer	The time remaining before the local router acts on an (S,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.
Join Expiry Timer	The time remaining before (S,G) Join state for this interface expires.
Assert State	The (S,G) Assert state for this interface. The possible values include No Info, Winner, or Loser.
Assert Timer	If Assert State is Winner, this is the time remaining before the local router sends a (S,G) Assert message on this interface. If the Assert State is Loser, this is the time remaining before the (S,G) Assert state expires.
Assert Winner	If the Assert State is Loser, this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is Loser, this is the metric preference of the route to the source advertised by the assert winner.
Assert Winner Metric Metric	If the Assert State is Loser, this is the routing metric of the route to the source advertised by the assert winner.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim groute	Displays (*,G) routing table entries for IPv6 PIM.

MIB Objects

```
pimSGTable
   pimSGAddressType
   pimSGGrpAddress
   pimSGSrcAddress
   pimSGUpTime
   pimSGPimMode
   pimSGUpstreamJoinState
   pimSGUpstreamJoinTimer
   pimSGUpstreamNeighbor
   pimSGRPFIfIndex
   pimSGRPFNextHopType
   pimSGRPFNextHop
   pimSGRPFRouteProtocol
   pimSGRPFRouteAddress
   pimSGRPFRoutePrefixLength
   pimSGRPFRouteMetricPref
   pimSGRPFRouteMetric
   pimSGSPTBit
   pimSGKeepaliveTimer
   pimSGDRRegisterState
   pimSGDRRegisterStopTimer
   pimSGRPRegisterPMBRAddressType
   pimSGRPRegisterPMBRAddress
   pimSGUpstreamPruneState
   pimSGUpstreamPruneLimitTimer
   pimSGOriginatorState
   pimSGSourceActiveTimer
   pimSGStateRefreshTimer
pimSGITable
   pimSGIIfIndex
   pimSGIUpTime
   pimSGILocalMembership
   pimSGIJoinPruneState
   pimSGIPrunePendingTimer
   pimSGIJoinExpiryTimer
   pimSGIAssertState
   pimSGIAssertTimer
   pimSGIAssertWinnerAddressType
   pimSGIAssertWinnerAddress
   pimSGIAssertWinnerMetricPref
   pimSGIAssertWinnerMetric
```

show ipv6 pim df-election

Displays the Designated Forwarder (DF) election state for Rendezvous Point (RP) interfaces. This command applies only to RPs operating in the Bidirectional PIM (BIDIR-PIM) mode.

show ipv6 pim df-election [*rp_address* | *if_name***]**

Syntax Definitions

rp_address	An IPv6 RP address.
if_name	The interface name.

Defaults

By default, the DF election state for all RP interfaces.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- When the *rp_address* is specified in the command line, only those interfaces associated with the specified RP address are displayed.
- When the *if_name* is specified in the command line, only information associated with the specified interface is displayed.

Examples

```
-> show ipv6 pim df-election
RP Address Interface Name DF State Winner Address          Uptime      Metric Metric Expires
                                                                       Pref
----------+--------------+--------+-----------------------------------+------+------+--------
2000::8    vlan-13        Win     fe80::220:daff:fe11:2233 00h:10m:15s 1      1   00h:00m:13s
           vlan-210       Win     fe80::220:daff:fe11:2233 00h:10m:15s 1      1   00h:00m:13s
2100::8    vlan-13        Win     fe80::220:daff:fe11:2233 00h:10m:15s 1      1   00h:00m:03s
           vlan-210       Win     fe80::220:daff:fe11:2233 00h:10m:15s 1      1   00h:00m:03s

-> show ipv6 pim df-election 2000::8
RP Address Interface Name DF State Winner Address          Uptime      Metric Metric Expires
                                                                       Pref
----------+--------------+--------+----------------------+-----------+------+------+--------
2000::8    vlan-13        Win     fe80::220:daff:fe11:2233 00h:10m:15s 1      1   00h:00m:13s
           vlan-210       Win     fe80::220:daff:fe11:2233 00h:10m:15s 1      1   00h:00m:13s

-> show ipv6 pim df-election vlan-13
RP Address Interface Name DF State Winner Address          Uptime      Metric Metric Expires
                                                                       Pref
----------+--------------+--------+----------------------+-----------+------+------+--------
2000::8    vlan-13        Win     fe80::220:daff:fe11:2233 00h:10m:15s 1      1   00h:00m:13s
2100::8    vlan-13        Win     fe80::220:daff:fe11:2233 00h:10m:15s 1      1   00h:00m:03s
```

output definitions

RP Address	The IPv6 address of the Rendezvous Point (RP).
Interface Name	The name of the IPv6 interface.
DF State	The state of the DF election process (**Offer**, **Lose**, **Win**, or **Backoff**).
Winner Address	The primary IPv6 address of the winner of the DF election process.
UpTime	The amount of time since the current winner was last elected the DF for the RP.
Metric Pref	The metric preference advertised by the DF winner. This value is zero if there currently is no DF.
Metric	The metric value advertised by the DF winner. This value is zero if there currently is no DF.
Expires	The minimum time remaining before the local router expires the current DF state.

Release History

Release 7.3.4; command was introduced.

Related Commands

show ipv6 pim interface	Displays detailed PIM settings for a specific interface.

MIB Objects

```
pimBidirDFElectionTable
   pimBidirDFElectionAddressType
   pimBidirDFElectionRPAddress
   pimBidirDFElectionIfIndex
   pimBidirDFElectionWinnerAddressType
   pimBidirDFElectionWinnerAddress
   pimBidirDFElectionWinnerUpTime
   pimBidirDFElectionWinnerMetricPref
   pimBidirDFElectionWinnerMetric
   pimBidirDFElectionState
   pimBidirDFElectionStateTimer
```

34 Multicast Routing Commands

This chapter describes multicast routing commands. Multicast routing is used in conjunction with IP Multicast Switching (IPMS). IPMS can operate either with or without multicast routing. However, for multicast routing to function, IPMS must be configured.

Multicast uses Class D IP addresses in the range 224.0.0.0 to 239.255.255.255. Addresses in the range 239.0.0.0 to 239.255.255.255 are reserved for boundaries, which are used to prevent multicast traffic from being forwarded on a VLAN group or network.

IP multicast routing is a way of controlling multicast traffic across networks. The multicast router discovers which networks want to receive multicast traffic by sending out Internet Group Management Protocol (IGMP) queries and receiving IGMP reports from attached networks. The IGMP reports signal that users want to join or leave a multicast group. If there is more than one multicast router in the network, the router with the lowest IP address is elected the querier router, which is responsible for querying the subnetwork for group members.

The current release also provides support for IPv6 multicast addresses. In the IPv6 addressing scheme, multicast addresses begin with the prefix ff00::/8. Similar to IPv6 unicast addresses, IPv6 multicast addresses also have different scopes depending on their prefix, though the range of possible scopes is different.

Multicast Listener Discovery (MLD) is the protocol used by an IPv6 router to discover the nodes which request multicast packets on its directly attached links and the multicast addresses that are of interest to those neighboring nodes. MLD is derived from version 2 of IPv4's Internet Group Management Protocol, IGMPv2. MLD uses ICMPv6 message types, rather than IGMP message types.

MIB information for the multicast routing commands is as follows:

Filename: ALCATEL-IND1-IPMRM-MIB.mib
Module: alcatelIND1IPMRMMIB

Filename: IPMCAST-MIB.mib
Module: ipMcastMIB

A summary of the available commands is listed here:

ip mroute-boundary
ip mroute-boundary extended
ip mroute interface ttl
ip mroute mbr
show ip mroute-boundary
show ip mroute
show ip mroute interface
show ip mroute-nexthop
show ip mroute mbr
ipv6 mroute interface ttl
show ipv6 mroute
show ipv6 mroute interface
show ipv6 mroute-nexthop

ip mroute-boundary

Adds or deletes scoped multicast address boundaries for a router interface. When a user on the specified interface joins the multicast group as defined by the scoped address—plus the mask length—all multicast traffic will stop being forwarded on that interface. This provides a mechanism for the end user to control multicast traffic from the network.

Refer to the "Configuring Multicast Address Boundaries" chapter in the *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide* for detailed information.

ip mroute-boundary *if_name scoped_address mask*

no ip mroute-boundary *if_name scoped_address mask*

Syntax Definitions

if_name	The interface name on which the boundary is being assigned.
scoped_address	A scoped multicast address identifying the group range for the boundary. Scoped addresses may range from 239.0.0.0–239.255.255.255.
mask	A corresponding Class A, B, or C mask address (e.g., 255.0.0.0).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to delete the scoped multicast address boundaries for a router interface.

Examples

```
-> ip mroute-boundary vlan-2 239.0.0.0 255.0.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip mroute-boundary	Displays scoped multicast address boundaries for the switch's router interfaces.

MIB Objects

```
ipMcastBoundaryTable
   ipMcastBoundaryIfIndex
   ipMcastBoundaryAddressType
   ipMcastBoundaryAddress
   ipMcastBoundaryAddressPrefixLength
```

ip mroute-boundary extended

Enables or disables the multicast route boundary expansion feature. On enabling the multicast route boundary is extended to all the multicast groups (that is, the non-scoped address, 224.0.0.0 to 239.255.255.255). All multicast traffic will stop being forwarded on that interface. This provides a mechanism for the end user to control multicast traffic from the network.

Refer to the "Configuring Multicast Address Boundaries" chapter in the applicable *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide* for detailed information.

ip mroute-boundary extended {enable | disable}

Syntax Definitions

enable	The multicast route boundary is extended to all the multicast cast address groups (224.0.0.0 through 239.255.255.255).
disable	The multicast route boundary is limited to administratively scoped multicast address (239.0.0.0 through 239.255.255.255).

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ip mroute-boundary extended enable
-> ip mroute-boundary extended disable
```

Release History

Release 8.2.1; command introduced.

Related Commands

show ip mroute-boundary	Displays multicast address boundaries for the switch's router interfaces.

MIB Objects

```
alaIpmrmGlobalConfig
   alaIpmrmExtendedBoundaryStatus
```

ip mroute interface ttl

Specifies a multicast datagram Time to Live (TTL) threshold for an existing router interface. IP multicast datagrams with a TTL value lower than the specified TTL threshold value will not be forwarded out of the interface.

ip mroute interface *if_ name* **ttl** *threshold*

Syntax Definitions

if_name	The interface name that has one of the Multicast routing protocols running (either DVMRP or PIM).
threshold	The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded out of the interface.

Defaults

parameter	default
threshold	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ip mroute interface vlan-1 ttl 255
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip mroute interface	Displays IP multicast interface information.

MIB Objects

```
alaIpMcastInterfaceTable
   alaIpMcastInterfaceIfIndex
   alaIpMcastInterfaceTtl
```

ip mroute mbr

Configures the switch to serve as a Multicast Border Router (MBR) that will provide interoperability between DVMRP and PIM domains.

ip mroute mbr admin-state {enable | disable}

Syntax Definitions

enable	Enables MBR functionality on the switch.
disable	Disables MBR functionality on the switch.

Defaults

MBR functionality is disabled by default.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- To configure the switch to operate as an MBR, first configure the DVMRP and PIM protocols for the switch then enable MBR functionality.
- The MBR functionality is operationally enabled only when there is at lease one PIM interface and one DVMRP interface enabled and both interfaces are operationally active on the switch.
- The MBR feature only supports interoperability between DVMRP and PIM (includes PIM-DM and PIM-SM) domains; no other routing protocols are supported.
- The following is *not* supported by the MBR feature in the current release:
  - PIM-SSM
  - Interoperability between multiple PIM domains
  - IPv6 (only IPv4)

Examples

```
-> ip mroute mbr admin-state enable
-> ip mroute mbr admin-state disable
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show ip mroute mbr	Displays MBR configuration information.

MIB Objects

`alaIpmrmMbrStatus`

ipv6 mroute interface ttl

Specifies a multicast datagram Time to Live (TTL) threshold for an existing IPv6 interface. Any IP multicast datagrams with a TTL value lower than the specified TTL threshold value will not be forwarded out of the interface.

ipv6 mroute interface *if_name* **ttl** *threshold*

Syntax Definitions

if_name	The name of the IPv6 interface.
threshold	The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded out of the interface.

Defaults

parameter	default
threshold	0

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ipv6 mroute interface vlan-1 ttl 255
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 mroute interface	Displays IPv6 multicast interface information.

MIB Objects

```
alaIpMcastInterfaceTable
   alaIpMcastInterfaceIfIndex
   alaIpMcastInterfaceTtl
```

show ip mroute-boundary

Displays scoped multicast address boundaries for the switch's router interfaces.

show ip mroute-boundary

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip mroute-boundary
Extended Boundary Address Range: enabled

Interface Name  Interface Address  Boundary Address
--------------+------------------+------------------
vlan-4           214.0.0.7          239.1.1.1/32
vlan-2           170.2.0.1          224.2.2.2/24
```

output definitions

Extended Boundary Address Range	Displays the status of extended multicast route boundary on the interface.
Interface Name	The name of the interface on which the boundary is assigned. Packets with a destination address in the associated address/mask range will not be forwarded from this interface.
Interface Address	The IP address of this interface where the boundary is assigned.
Boundary Address	The scoped multicast address that, when combined with the boundary mask, identifies the scoped boundary range. The boundary's subnet mask is shown using the CIDR prefix length: 255.0.0.0 equals /8; 255.255.0.0 equals /16; 255.255.255.0 equals /24.

Release History

Release 7.1.1; command was introduced.
Release 8.2.1; **Extended Boundary Address Range** output filed added.

Related Commands

ip mroute-boundary	Adds or deletes a router's scoped multicast address boundaries.
ip mroute interface ttl	Enables or disables the multicast route boundary expansion feature.
show ip mroute interface	Displays IP multicast interface information.

MIB Objects

```
ipMcastBoundaryTable
   ipMcastBoundaryIfIndex
   ipMcastBoundaryAddressType
   ipMcastBoundaryAddress
   ipMcastBoundaryAddressPrefixLength
   ipMcastBoundaryStatus
alaIpmrmGlobalConfig
   alaIpmrmExtendedBoundaryStatus
```

show ip mroute

Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

show ip mroute

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip mroute

Total 2 Mroutes
Group Address   Src Address      Upstream Nbr    Route Address      Proto
--------------+---------------+---------------+----------------+----------
225.0.0.0       214.0.0.2/32      0.0.0.0       214.0.0.0/24        PIM-SM
225.0.0.1       214.0.0.2/32      0.0.0.0       214.0.0.0/24        PIM-DM
```

output definitions

Group Address	The IP multicast group address for this entry.
Src Address	The network address which identifies the source for this entry.
Upstream Nbr	The address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received.
Route Address	The address portion of the route used to find the upstream or parent interface for this multicast forwarding entry.
Proto	The multicast routing protocol through which this multicast forwarding entry was learned (i.e., DVMRP, PIM-SM or PIM-DM).

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip mroute interface	Displays IP multicast interface information.
show ip mroute-nexthop	Displays IP next-hop information on outgoing interfaces for routing IP multicast datagrams.

MIB Objects

```
alaIpMcastRouteTable
   alaIpMcastRouteGroup
   alaIpMcastRouteSource
   alaIpMcastRouteInIfIndex
   alaIpMcastRouteUpstreamNeighbor
   alaIpMcastRouteRtAddress
   alaIpMcastRouteRtPrefixLength
   alaIpMcastRouteProtocol
```

show ipv6 mroute

Displays multicast routing information for IPv6 datagrams sent by particular sources to the IPv6 multicast groups known to this router.

show ipv6 mroute

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 mroute
Total 2 Mroutes
Group Address Source Address Interface Upstream Neighbor Route Addr/PrefixLen Proto
------------+---------------+---------+----------------------+--------------+-----
ff06:7777::1 2600::7         vlan-30  fe80::2d0:95ff:feac:a537 2600::/64     PIM-SM
ff06:7777::2 2600::7         vlan-30  fe80::2d0:95ff:feac:a537 2600::/64     PIM-SM
```

output definitions

Group Address	The IPv6 multicast group address for this entry.
Source Address	The IPv6 multicast address, which identifies the source for this entry.
Interface	The name of the IPv6 interface on which the datagrams sent by these sources to this IPv6 multicast address are received.
Upstream Neighbor	The IPv6 address of the upstream neighbor from which the datagrams from these sources to this multicast address are received.
Route Addr/Prefix len	The IPv6 address portion of the route used to find the upstream or parent interface for this IPv6 multicast forwarding entry.
Proto	The IPv6 multicast routing protocol through which this IPv6 multicast forwarding entry was learned.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 mroute interface	Displays IPv6 multicast interface information.
show ipv6 mroute-nexthop	Displays IPv6 next-hop information on outgoing interfaces for routing IPv6 multicast datagrams.

MIB Objects

```
alaIpMcastRouteTable
   alaIpMcastRouteGroup
   alaIpMcastRouteSource
   alaIpMcastRouteInIfIndex
   alaIpMcastRouteUpstreamNeighbor
   alaIpMcastRouteRtAddress
   alaIpMcastRouteRtPrefixLength
   alaIpMcastRouteProtocol
```

show ip mroute interface

Displays IP multicast interface information.

show ip mroute interface [*interface_name***]**

Syntax Definitions

interface_name	The name of the interface

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Not specifying an interface name displays all known IP multicast interfaces information.

Examples

```
-> show ip mroute interface

Interface Name     IP Address     TTL   Multicast Protocol
---------------+---------------+------+--------------------
vlan-4             214.0.0.7       0        PIM
vlan-26            172.21.63.7     0        PIM
vlan-11            212.61.11.7     0        PIM
```

output definitions

Interface Name	The name configured for the interface.
IP Address	The IP address of this interface entry.
TTL	The datagram TTL threshold for the interface. Any IP multicast datagrams with a TTL less than the threshold displayed in the table will not be forwarded out of the interface. The default value, 0, specifies that *all* multicast packets are forwarded out of the interface.
Multicast Protocol	The multicast routing protocol currently running on this interface. Options include DVMRP and PIM.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip mroute	Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.
show ip mroute-nexthop	Displays IP next-hop information on outgoing interfaces for routing IP multicast datagrams.

MIB Objects

```
alaIpMcastInterfaceTable
   alaIpMcastInterfaceIfIndex
   alaIpMcastInterfaceTtl
   alaIpMcastInterfaceProtocol
```

show ipv6 mroute interface

Displays IPv6 multicast interface information.

show ipv6 mroute interface {*interface_name***}**

Syntax Definitions

interface_name	The name of the interface

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Not specifying an interface name displays all known IPv6 multicast interfaces information.

Examples

```
-> show ipv6 mroute interface

Interface Name     IP Address     TTL   Multicast Protocol
---------------+---------------+------+--------------------
vlan-4             2000::1      0        PIM
vlan-26            2000::2      0        PIM
vlan-11            2000::3      0        PIM
```

output definitions

Interface Name	The name configured for the IPv6 interface.
IP Address	The IPv6 address of this interface entry.
TTL	The datagram TTL threshold for the interface. Any IPv6 multicast datagrams with a TTL less than the threshold displayed in the table will not be forwarded out of the interface. The default value, 0, specifies that *all* multicast packets are forwarded out of the interface.
Multicast Protocol	The multicast routing protocol currently running on this interface. Options include DVMRP and PIM.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 mroute	Displays multicast routing information for IPv6 datagrams sent by particular sources to the IPv6 multicast groups known to this router.
show ipv6 mroute-nexthop	Displays IPv6 next-hop information on outgoing interfaces for routing IPv6 multicast datagrams.

MIB Objects

```
alaIpMcastInterfaceTable
   alaIpMcastInterfaceIfIndex
   alaIpMcastInterfaceTtl
   alaIpMcastInterfaceProtocol
```

show ip mroute-nexthop

Displays next-hop information on outgoing interfaces for routing IP multicast datagrams.

show ip mroute-nexthop

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ip mroute-nexthop

Total 10 Nexthops

Group Address  Src Address   Interface Name    Next Hop     Protocol
                                               Address
-------------+-------------+----------------+-------------+----------
225.0.0.0     214.0.0.2/32      vlan-26        225.0.0.0    PIM-SM
225.0.0.1     214.0.0.2/32      vlan-26        225.0.0.1    PIM-SM
225.0.0.2     214.0.0.2/32      vlan-26        225.0.0.2    PIM-SM
225.0.0.3     214.0.0.2/32      vlan-26        225.0.0.3    PIM-SM
225.0.0.4     214.0.0.2/32      vlan-26        225.0.0.4    PIM-SM
225.0.0.5     214.0.0.2/32      vlan-26        225.0.0.5    PIM-SM
225.0.0.6     214.0.0.2/32      vlan-26        225.0.0.6    PIM-SM
225.0.0.7     214.0.0.2/32      vlan-26        225.0.0.7    PIM-SM
225.0.0.8     214.0.0.2/32      vlan-26        225.0.0.8    PIM-SM
225.0.0.9     214.0.0.2/32      vlan-26        225.0.0.9    PIM-SM
```

output definitions

Group Address	The IP multicast group address for this entry.
Src Address	The network address, which identifies the source for this entry.
Interface Name	Generally, this is the name configured for the interface.
Next Hop Address	The address of the next-hop that is specific to this entry.
Protocol	The routing protocol by which this next-hop was learned (i.e., DVMRP or PIM-SM).

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip mroute	Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.
show ip mroute interface	Displays IP multicast interface information.

MIB Objects

```
alaIpMcastRouteNextHopTable
   alaIpMcastRouteNextHopGroup
   alaIpMcastRouteNextHopSource
   alaIpMcastRouteNextHopIfIndex
   alaIpMcastRouteNextHopAddress
   alaIpMcastRouteNextHopProtocol
```

show ipv6 mroute-nexthop

Displays IPv6 next-hop information on outgoing interfaces for routing IPv6 multicast datagrams.

show ipv6 mroute-nexthop

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ipv6 mroute-nexthop
Total 2 Nexthops
Group Address   Source Address    Interface    Next Hop Address        Protocol
---------------+-----------------+-----------+-----------------------+---------
ff06:7777::1    2600::7           vlan-40      ff06:7777::1            PIM-SM
ff06:7777::2    2600::7           vlan-40      ff06:7777::2            PIM-SM
```

output definitions

Group Address	The IPv6 multicast group address for this entry.
Src Address	The IPv6 multicast address, which identifies the source for this entry.
Interface Name	The name of the IPv6 interface on which the datagrams sent by these sources to this IPv6 multicast address are received.
Next Hop Address	The IPv6 address of the next-hop that is specific to this entry.
Protocol	The IPv6 multicast routing protocol by which this IPv6 multicast forwarding entry was learned.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 mroute	Displays multicast routing information for IPv6 datagrams sent by particular sources to the IPv6 multicast groups known to this router.
show ipv6 mroute interface	Displays IPv6 multicast interface information.

MIB Objects

```
alaIpMcastRouteNextHopTable
   alaIpMcastRouteNextHopGroup
   alaIpMcastRouteNextHopSource
   alaIpMcastRouteNextHopIfIndex
   alaIpMcastRouteNextHopAddress
   alaIpMcastRouteNextHopProtocol
```

show ip mroute mbr

Displays the MBR status for the switch.

show ip mroute mbr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

The MBR feature only supports interoperability between DVMRP and PIM. Both of these multicast protocols must be configured and operationally active on the switch.

Examples

```
-> show ip mroute mbr
MBR Status                      = enabled,
Protocols Registered            = DVMRP PIM
```

output definitions

MBR Status	The administrative status (**enabled** or **disabled**) of MBR functionality on the switch.
Protocols Registered	The operationally active multicast protocols (**DVMRP**, **PIM**) to which MBR functionality is applied.

Release History

Release 7.3.2; command was introduced.

Related Commands

ip mroute mbr	Configures the administrative status of Multicast Border Router functionality.

MIB Objects

```
alaIpmrmGlobalConfig
   alaIpmrmMbrStatus
   alaIpmrmMbrProtocolApps
```

35 QoS Commands

The OmniSwitch QoS software provides a way to manipulate flows coming through the switch based on user-configured policies. The flow manipulation (generally referred to as *Quality of Service* or *QoS*) may be as simple as allowing/denying traffic, or as complicated as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

This chapter provides information about configuring QoS global and port parameters through the Command Line Interface (CLI). Refer to Chapter 44, "QoS Policy Commands," for information about commands used to configure QoS policy rules.

MIB information for the QoS commands is as follows:

Filename: ALCATEL-IND1-QOS-MIB.mib
Module alaQoSMIB

Filename: ALCATEL-IND1-VIRTUAL-FLOW-CONTROL-MIB.mib
Module alcatelIND1VfcMIB

Important Note. Some of the commands listed here are not currently supported on one or more platforms. See command descriptions in this chapter and check release notes for information about commands that are not supported.

The QoS commands are listed here:

Global commands	**qos** **qos trust-ports** **qos forward log** **qos log console** **qos log lines** **qos log level** **qos stats interval** **qos phones** **qos quarantine mac-group** **qos user-port** **qos dei** **debug qos** **debug qos internal** **clear qos log** **qos apply** **qos revert** **qos flush** **qos reset** **qos stats reset** **qos switch-group** **show qos slice** **show qos log** **show qos config** **show qos statistics**

Port and Slice commands	**qos port** **qos port reset** **qos port trusted** **qos port maximum egress-bandwidth** **qos port maximum ingress-bandwidth** **qos port maximum depth** **qos port default 802.1p** **qos port default dscp** **qos port default classification** **qos port dei** **show qos port**
Queue Management commands	**qos qsp import** **qos qsp qp** **qos qsi qsp** **qos qsp system-default** **qos qsi stats** **show qos qsi summary** **show qos qsp** **show qos wrp** **show qos qsi** **show qos qsi stats** **show qos qsi wred-stats** **show qos qsp system-default** **clear qos qsi stats**
Data Center Bridging commands	**qos qsp dcb import** **qos qsp dcb tc** **qos qsp dcb tc-numbering** **qos qsi qsp dcb** **qos qsi dcb dcbx version** **qos qsi dcb dcbx admin-state** **qos qsi dcb dcbx ets** **qos qsi dcb dcbx pfc** **show qos qsi summary** **show qos qsp dcb** **show qos qsi dcb dcbx** **show qos qsi dcb ets** **show qos qsi dcbx pfc** **show qos pfc-lossless-usage** **show qos qsi dcb pfc stats** **show qos qsi stats** **clear qos qsi stats** **clear qos qsi dcb pfc stats**

qos

Enables or disables QoS. This section describes the base command with a single required option (**enable** or **disable**).

In lieu of this option, the base command (**qos**) may be used with other keywords to set up global QoS configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

qos {enable | disable}
[trust-ports]
[forward log]
[log console]
[log lines *lines***]**
[log level *level***]**
[stats interval *seconds***]**
[phones [priority *priority_value* **| trusted]]**
[user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcpserver | dns-reply}]

Syntax Definitions

enable	Enables QoS. The QoS software in the switch classifies flows coming into the switch to attempt to match them to QoS policies. If a match is found, the policy parameters are applied to the flow. The **enable** setting may be used alone or in conjunction with optional command keywords.
disable	Disables QoS. Flows coming into the switch are not matched to policies. The **disable** setting cannot be used with any other command keyword.

Defaults

parameter	default
enable | **disable**	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When QoS is disabled, flows coming into the switch are classified but not matched to a policy. Traffic is treated as best effort and assigned to default queues.
- The command keywords may be used with or without **enable**; these keywords cannot be used with **disable**.

Examples

```
-> qos disable
-> qos enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy rule	Configures a policy rule on the switch.
show policy rule	Displays information for policy rules configured on the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigEnable
   alaQoSConfigTrustedPorts
   alaQoSConfigForwardLog
   alaQoSConfigLogLines
   alaQoSConfigLogLevel
   alaQoSConfigLogConsolealaQoSConfigStatsInterval
   alaQoSConfigAutoPhones
   alaQoSConfigUserportFilter
   alaQoSConfigAppliedUserportFilter
   alaQoSConfigUserportShutdown
   alaQoSConfigAppliedUserportShutdown
```

qos trust-ports

Configures the global trust mode for QoS ports. Trusted ports can accept 802.1p and ToS/DSCP values in incoming packets; untrusted ports will set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured.

Any port configured through the **qos port** command will automatically be added in the trust mode specified by this command. See page 35-35 for more information about this command.

qos trust-ports

qos no trust-ports

Syntax Definitions

N/A

Defaults

By default, all ports are untrusted.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **qos ports trusted** command to override the default for a particular port.
- The setting only applies to ports with incoming traffic.
- Mobile ports are always trusted regardless of the global setting.
- Use the **qos port default 802.1p** or **qos port default dscp** commands to specify that a value other than zero should be applied to the incoming packets. Note that this value is overridden if a policy exists that specifies a different value for such packets.

Examples

```
-> qos trust-ports
-> qos no trust-ports
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port trusted	Configures whether or not a particular port is trusted or untrusted.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigTrustedPorts
```

qos forward log

Enables the QoS software in the switch to send events to the policy server software in the switch in real time. The policy server software may then be polled by an NMS application for logged events.

qos forward log

qos no forward log

Syntax Definitions

N/A

Defaults

By default, logged events are not sent to the policy server software in the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

An NMS application may query the Policy Manager in the switch for logged events. Use the **qos forward log** command to forward each event as it happens.

Examples

```
-> qos forward log
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigForwardLog
```

qos log console

Sends QoS log messages to the switch logging utility, which is an event logging application available on the OmniSwitch. The configuration of the switch logging utility determines if QoS messages are sent to a log file in the switch's flash file system, displayed on the switch console, or sent to a remote syslog server.

qos log console

qos no log console

Syntax Definitions

N/A

Defaults

QoS log messages are not sent to the switch logging utility by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To display QoS log events as they happen on an output console attached to the switch, configure the switch logging utility to output events to the console. This is done using the **swlog output** command.
- The entire log may be viewed at any time using the **show qos log** command.

Examples

```
-> qos log console
-> qos no log console
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
swlog output	Enables or disables switch logging output to the console, file, or data socket (remote session).
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigLogConsole
```

qos log lines

Configures the number of lines in the QoS log.

qos log lines *lines*

Syntax Definitions

lines	The number of lines included in the QoS log. A value of zero turns off logging to the console. The range is 0–10240.

Defaults

parameter	default
lines	10240

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To turn off logging, enter 0 for the number of log lines. (Note that error messages will still be logged.)
- If you change the number of log lines, you may clear all messages in the QoS log. To avoid clearing all messages in the log, enter the **qos log lines** command in the **boot.cfg** file. The log length will be changed at the next reboot.

Examples

```
-> qos log lines 5
-> qos log lines 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigLogLines
```

qos log level

Configures the level of log detail.

qos log level *level*

qos no log level

Syntax Definitions

level	The level of log detail, ranging from 1 (least detail) to 8 (most detail).

Defaults

parameter	default
level	5

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **debug qos** command to change the type of debugging messages that are logged. The **qos log level** command configures the level of detail for these messages.
- If the **debug qos** command is not configured to log any kind of information (this is the default), the **qos log level** command has no effect.
- Note that a high log level value will impact the performance of the switch.

Examples

```
-> qos log level 4
-> qos log level 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigLogLevel
```

qos stats interval

Configures how often the switch polls network interfaces for statistics about QoS events.

qos stats interval *seconds*

Syntax Definitions

seconds	The number of seconds before the switch polls network interfaces for statistics. The range is 1–3600.

Defaults

parameter	default
seconds	60

Platforms Supported

Not supported in this release.

Usage Guidelines

- Change the statistics interval to a smaller interval if you want to monitor QoS events.
- Change the statistics interval to a larger interval if you want to free some switch memory.

Examples

```
-> qos stats interval 30
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; command deprecated, interval set to 5 seconds.

Related Commands

show qos statistics	Displays statistics about the QoS configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigStatsInterval
```

qos phones

Enables or disables the automatic prioritization of IP phone traffic.

qos phones [priority *priority_value* **| trusted]**

qos no phones

Syntax Definitions

priority_value	The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).
trusted	Trusts IP phone traffic; priority value of the IP phone packet is used.

Defaults

parameter	default
priority_value **| trusted**	trusted

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable automatic prioritization of IP phone traffic.
- IP phone traffic is identified by examining the source MAC address of the packet received on the port. If the source MAC falls within one of the following ranges, the QoS IP phone priority is automatically assigned to the MAC:

MAC Address Range	Description
00:80:9f:00:00:00—00:80:9f:ff:ff:ff	Enterprise IP Phones Range
78:81:02:00:00:00—78:81:02:ff:ff:ff	Communications IP Phones Range
00:13:fa:00:00:00—00:13:fa:ff:ff:ff	Lifesize IP Phones Range
48:7a:55:00:00:00—48:7a:55:ff:ff:ff	ALE 8008 IP Phone MAC Range

- To automatically apply the QoS IP phone priority to other, non-IP phone traffic, add the source MAC addresses of such traffic to the QoS “alaPhone” group.
- When automatic prioritization of IP phone traffic is enabled, QoS policies that specify priority are not applied to the IP phone traffic. Other QoS policies, however, are applied to this type of traffic as usual.
- On the OmniSwitch 6860, consider the following:
  - When automatic prioritization of QoS IP phone traffic is enabled, a rule is configured in the FFP (Fast Filtering Processor) with the source MAC address as 00:80:9F:00:00:00 and the mask FF:FF:FF:00:00:00 and 00-13-FA-xx-xx-xx and mask FF:FF:FF:00:00:00.
  - The QoS IP phone prioritization and SIP Snooping features are mutually exclusive. If one of these features is enabled when an attempt is made to enable the other feature, an error message is displayed. To enable QoS IP phone prioritization, first use the **sip-snooping admin-state disable**

command to disable SIP Snooping. To enable the SIP Snooping feature, first use the **qos no phones** command to disable QoS IP phone prioritization.

Note. Note. QoS IP phone prioritization is configured, by default, on initialization

Examples

```
-> qos phones priority 7
-> qos phones trusted
-> qos no phones
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; additional IP phone MAC ranges added.

Related Commands

show qos config	Displays the QoS configuration for the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigAutoPhones
```

qos quarantine mac-group

Configures the name of the Quarantine MAC address group. The OmniVista Quarantine Manager application identifies source MAC addresses to quarantine and adds these addresses to the Quarantine MAC group.

qos quarantine mac-group *mac_group*

qos no quarantine mac-group

Syntax Definitions

mac_group	The name of the Quarantine MAC group (up to 31 alphanumeric characters).

Defaults

By default, the quarantine MAC group is not configured on the switch.

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

- Use the **no** form of the command to reset the default MAC group name back to “Quarantined”.
- The *mac_group* name specified with this command must match the group name specified with the OmniVista Quarantine Manager application.
- Each switch can have a different Quarantine MAC group name as long as each switch matches the OmniVista Quarantine Manager MAC group name for that switch. Note that there is only one such MAC group per switch.
- Do not use the Quarantine MAC group name in regular QoS policies.
- This group is also used by the switch Quarantine Manager and Remediation (QMR) application to restrict or restore network access to quarantined MACs.
- Note that QMR is not available if VLAN Stacking services or QoS VLAN Stacking inner VLAN and 802.1p policies are configured on the switch.
- QMR is considered active when there are MAC addresses in the Quarantine MAC address group. Use the **show quarantine mac group** command to display the contents of this group. In addition, the **show mac-learning** command output display identifies quarantined MAC addresses.

Examples

```
-> qos quarantine mac-group mac_group1
-> no quarantine mac-group
```

Release History

Release 8.1.1; command was introduced.

Related Commands

qmr quarantine path	Specifies the URL for a remediation server.
qmr quarantine page	Configures the Quarantine Manager and Remediation (QMR) application to send a Quarantined page to a client if a remediation server is not configured.
show quarantine mac group	Displays information about the Quarantine MAC group.
show qmr	Displays the QMR configuration for the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigQuarantineMacGroupName
```

qos user-port

Configures the option to filter packets or administratively disable a port when the specified type of traffic is received on a port that is a member of the pre-defined UserPorts group.

qos user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}

qos no user-port {filter | shutdown}

Syntax Definitions

filter	Filters the specified type of traffic when it is received on UserPort ports.
shutdown	Administratively disables UserPort ports that receive the specified type of traffic.
spoof	Detects IP spoofing. The source IP address of a packet ingressing on a user port is compared to the subnet of the VLAN for the user port; the packet is dropped if these two items do not match. Also applies to ARP packets.
bgp	Filters only BGP protocol packets from a TCP session that was not originated by the same switch that has this filter configured.
bpdu	Filters conventional Spanning Tree BPDU (destination MAC address 0x0180c2:000000) packets and GVRP (destination MAC address 0x0180c2:000021) packets.
rip	Filters RIP protocol packets.
ospf	Filters OSPF protocol packets.
vrrp	Filters VRRP protocol packets.
dvmrp	Filters IGMP packets with a type of 0x13. This applies only to IP packets with no options.
pim	Filters PIMv1, PIM-DM, and PIM-SM packets. The PIMv1 filter applies only to IP packets with no options.
isis	Filters IS-IS protocol packets.
dhcp-server	Filters response packets originating from a DHCP or BOOTP server that is configured on the known UDP port 67.
dns-reply	Filters all packets (both TCP and UDP) that originate from the known DNS port 53.

Defaults

parameter	default
filter	spoof
shutdown	none

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to disable the filter or shutdown function. This form of the command effects the overall operation of the feature.
- To specify more than one traffic type in the same command line, enter each type separated by a space (e.g., **spoof bgp ospf**).
- The **filter** option is applied only to ingress traffic on ports that are members of the UserPorts group. However, the switch will still process the filtered packets to determine if an egress update is sent on the same port. For example, if RIP traffic is filtered, the switch will still send RIP peer updates on that port.
- Note that existing traffic types to filter or shutdown are removed each time the **filter** or **shutdown** option is configured. Specify all desired traffic types each time the **qos user-port** command is performed to retain previously configured traffic types.
- No changes to the **filtering** and **shutdown** options are applied to the switch until the **qos apply** command is performed.
- This command only applies to ports that are members of the UserPorts group. Use the **policy port group** command to create and assign members to the UserPorts group.
- An SNMP trap is sent when a port is administratively disabled through a UserPorts shutdown function or a port disable action.
- To enable a port disabled by a user port shutdown operation, use the **interfaces admin** command to administratively enable the port or disconnect and reconnect the port cable.
- Up to 126 IP interfaces are supported with spoof detection on user ports. If the number of interfaces exceeds this amount, user port packets ingressing on those interfaces that exceed the 126 limit are dropped.
- To enforce anti-spoofing, a VLAN must have an IP address associated with it. If there is no IP address associated with the VLAN, no packets will be dropped.

Examples

```
-> qos user-port filter spoof bpdu
-> qos user-port shutdown spoof bgp ospf
-> qos no user-port shutdown
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; OmniSwitch 6560 support for **BPDU shutdown** added.

Related Commands

policy port group	Configures a port group and its associated slot and port numbers.
show qos config	Displays QoS configuration information.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigUserportFilter
   alaQoSConfigAppliedUserportFilter
   alaQoSConfigUserportShutdown
   alaQoSConfigAppliedUserportShutdown
```

qos dei

Configures the global Drop Eligible Indicator (DEI) bit mapping and marking setting for all QoS ports.The DEI setting applies to packets marked yellow (non-conforming) as the result of Tri-Color Marking (TCM) or other rate limiting mechanisms.

qos dei {ingress | egress}

qos no dei {ingress | egress}

Syntax Definitions

ingress	Maps the DEI/CFI bit to yellow (non-conforming) if this bit is set for ingress traffic. *DEI mapping is not supported on the OmniSwitch 6465.*
egress	Marks the DEI/CFI bit for egress packets if the packets were marked yellow as a result of the rate limiting process.

Defaults

By default, no DEI bit marking or mapping is done.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the global DEI bit mapping (ingress) or marking (egress) configuration for the switch.
- Use the **qos port dei** command to set the DEI bit mapping and marking configuration for a specific port. Note that the port setting takes precedence over the global DEI setting.
- Packets marked yellow by rate limiting are still transmitted when there is no congestion on the egress port queues. Setting the DEI bit for yellow egress packets (**qos dei egress**) ensures that an upstream switch is made aware that the packet was marked yellow.
- When a switch receives a yellow packet with the DEI bit set and ingress DEI bit mapping is enabled (**qos dei ingress**), the packet is mapped to an internal drop precedence or yellow color marking for the switch.
- DEI bit mapping is not supported on the OmniSwitch 6465. As a result, packets are processed as follows on that switch:
  - When packets are received on a trusted port, the DEI bit is retained only if the packets were not subject to a meter. If the port is untrusted, however, the DEI bit is always reset.
  - When a meter is set and DEI egress is configured on a trusted port, the DEI bit is reset to 0 for green packets. Yellow–red packets egress with the DEI bit set to 1.

Examples

```
-> qos dei ingress
-> qos dei egress
```

```
-> qos no dei ingress
-> qos no dei egress
```

Release History

Release 7.2.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port dei	Configures the Drop Eligible Indicator (DEI) bit mapping and marking setting for the specified QoS port.
policy action cir	Configures a Tri-Color Marking policy action.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDEIMapping
   alaQoSConfigDEIMarking
```

debug qos

Configures the type of QoS events that will be displayed in the QoS log.

debug qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress]

debug no qos

debug no qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress]

Syntax Definitions

info	Logs basic information about the switch.
config	Logs information about the global configuration.
rule	Logs events for rules configured on the switch.
main	Logs information about basic program interfaces.
port	Logs events related to QoS ports.
msg	Logs QoS messages.
sl	Logs information about source learning.
mem	Logs information about memory.
mapper	Logs information about mapping queues.
slot	Logs events related to slots.
l2	Logs Layer 2 QoS events on the switch.
l3	Logs Layer 3 QoS events on the switch.
classifier	Logs information whenever the switch classifies a flow; more details are provided if the log level is higher.
nat	*Not supported in this release.*
sem	Logs information about semaphore, process locking.
pm	Logs events related to the Policy Manager.
ingress	Logs information about packets arriving on the switch.
egress	Logs information about packets leaving the switch.

Defaults

By default basic information messages are logged (**info**). Error messages are always logged.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to change the type of messages that will be logged or to return debugging to its default state.

- Use this command to troubleshoot QoS events on the switch.

Examples

```
-> debug qos flows queue
-> qos debug no flows no queue
-> debug no qos
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos forward log	Enables the switch to send events to the PolicyView application in real time.
qos log lines	Configures the number of lines in the QoS log.
qos log level	Configures the level of log detail.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDebug
```

debug qos internal

Displays debugging information for QoS internal to the switch.

debug qos internal [slice *slot/slice***] [flow] [queue] [port] [l2tree] [l3tree] [vector] [pending] [verbose] [mapper] [pool] [log] [pingonly | nopingonly]**

Syntax Definitions

slot/slice	The slot number and slice to view debugging information. A *slice* is a logical section of hardware that corresponds to particular ports on a network interface module.
flow	Displays information about QoS flows.
queue	Displays information about QoS queues.
port	Displays information about QoS ports.
l2tree	Displays information about Layer 2 flows.
l3tree	Displays information about Layer 3 flows.
vector	Displays information about vectors.
pending	Displays information about pending QoS objects.
verbose	Sets the output to verbose mode for more detailed information.
mapper	Displays information about QoS mapping flows to queues.
pool	Displays information about the buffer pool.
log	Displays information about QoS information that is logged.
pingonly	Specifies that any policies configured with an ICMP protocol condition apply only to ICMP echo-requests and echo-replies.
nopingonly	Configures the switch so that any policies configured with an ICMP protocol condition apply to any ICMP packets.

Defaults

Debugging is disabled by default.

parameter	default
pingonly | nopingonly	**nopingonly**

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **debug qos** command to configure the type of QoS events that will be displayed in the QoS log.
- Use the **qos log level** command to set the level of log detail in the QoS log.

Examples

```
-> debug qos internal "verbose log"
```

Release History

Release 7.1.1; command was introduced.

Related Commands

debug qos	Configures the type of QoS events that will be displayed in the QoS log.
qos log level	Configures the level of log detail.

MIB Objects

N/A

clear qos log

Clears messages in the current QoS log.

clear qos log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command is useful for clearing messages from a large log file so that the file is easier to view. Logs can get large if invalid rules are configured on the switch, or if a lot of QoS events have taken place. Clearing the log makes the file easier to manage.

Examples

```
-> clear qos log
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigClearLog
```

qos apply

Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).

qos apply

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is required to activate all QoS and policy commands. This is the only command that causes current changes to be written to flash.
- Rules are configured through the **policy rule** command, but are not active on the switch until you enter **qos apply**.

Examples

```
-> qos apply
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos revert	Removes any policies configured through policy rule but not applied to the current configuration through the **qos apply** command.
qos reset	Resets the QoS configuration to its default values.
qos flush	Deletes all pending policy information.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigApply
```

qos revert

Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.

qos revert

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to remove currently configured policies that have not yet been activated through the **qos apply** command.

Examples

```
-> qos revert
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy rule	Configures a policy rule and saves it to the current configuration but does not make it active on the switch.
qos apply	Applies all QoS settings configured on the switch to the current configuration.
qos reset	Resets the QoS configuration to its defaults.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigRevert
```

qos flush

Deletes all pending policy information. This command is different from **qos revert**, which returns the pending policy configuration to its last applied settings.

qos flush

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If you enter this command, the pending policy configuration is completely erased. If you then enter **qos apply**, the erased configuration *overwrites the applied policies and you will erase all of your policy configuration.*

Note. Do not use this command unless you want to erase all of your policy configuration and start configuring new policies.

- Use the **qos revert** command to return the pending policy configuration to its last applied value.
- Policy configuration includes the following commands:

base commands	
policy rule	**policy mac group**
policy network group	**policy port group**
policy service	**policy condition**
policy service group	**policy action**

Examples

```
-> qos flush
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos revert	Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
policy server flush	Removes all cached LDAP policy data from the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigFlush
```

qos reset

Resets the QoS configuration to its defaults.

qos reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to reset QoS configuration that has not yet been applied through the **qos apply** command. The parameters are reset to their defaults.

Examples

```
-> qos reset
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies all QoS settings configured on the switch to the current configuration.
qos revert	Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigReset
```

qos stats reset

Resets QoS statistic counters to zero.

qos stats reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to reset global QoS statistics to zero. Statistics may be displayed with the **show qos statistics** command.

Examples

```
-> qos stats reset
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show qos statistics	Displays statistics about the QoS configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigStatsReset
```

qos switch-group

Changes how the switch handles IP addresses configured on the switch to help reduce the number of hardware entries required for QoS policies that use an IP address configured on the switch.

qos switch-group {expanded | compact}

Syntax Definitions

expanded	Uses the expanded method for populating the hardware routing table. This method requires a hardware entry for each individual IP interface belonging to either the built-in 'Switch' or 'Switch6' network groups.
compact	Uses the compact method for populating the hardware routing table by programming a single next hop entry for all IP interfaces belonging to either the built-in 'Switch' or 'Switch6' network groups.

Defaults

parameter	default
expanded | compact	**expanded**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- The **expanded** method can be used to reduce the hardware entries required and allow for a single hardware entry to be programmed for all the IP interfaces belonging to either the built-in 'Switch' or 'Switch6' network groups instead of a hardware entry for each individual IP address.
- The built-in policy network group 'Switch' contains all the IPv4 interfaces configured on the switch.
- The built-in policy network group 'Switch6' contains all the IPv6 interfaces configured on the switch.
- It is required to reboot the switch for the switch group setting to take effect. The current setting will always be shown, with the modified setting in parentheses in the **show qos config** command.

Examples

```
-> qos switch-group compact
-> qos switch-group expanded
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

show qos config	Displays global information about the QoS configuration.

MIB Objects

```
alaQoSConfig
   alaQoSConfigSwitchGroup
```

qos port reset

Resets all QoS port configuration to the default values.

qos port *chassis/slot/port***[**-*port2***] reset**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The QoS port configuration parameters that are reset include:

parameter	default
default queues	8
trusted	not trusted

Examples

```
-> qos port 3/1 reset
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortReset
```

qos port

Configures QoS parameters for a physical port. This section describes the base command with a single required option (*slot/port*).

In lieu of these options, the base command (**qos port**) may be used with other keywords to set up a QoS configuration on a per port basis. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

qos port *chassis/slot/port***[**-*port2***]**
[trusted]
[maximum egress-bandwidth *bps***]**
[maximum ingress-bandwidth *bps***]**
[maximum depth *bps***]**
[default 802.1p *value***]**
[default dscp *value***]**
[default classification {802.1p | tos | dscp}]

Syntax Definitions

chassis	The chassis identifier.
slot/port[-*port2*]	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

Defaults

- All ports are untrusted.
- By default, QoS ports do not preempt queues of lower priority.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **trusted** option to change the trust mode for the port.

Examples

```
-> qos port 3/1 trusted
-> qos port 4/2 no trusted
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port trusted	Configures whether the default mode for QoS ports is trusted or untrusted.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortTrusted
   alaQoSPortMaximumBandwidth
   alaQoSPortMaximumBandwidthStatus
   alaQoSPortMaximumIngBandwidth
   alaQoSPortMaximumIngBandwidthStatus
   alaQoSPortMaximumDefaultDepth
   alaQoSPortMaximumDefaultDepthStatus
   alaQoSPortDefault8021p
   alaQoSPortDefaultDSCPalaQoSPortDefaultClassification
```

qos port trusted

Configures whether an individual port is trusted or untrusted. Trusted ports can accept the 802.1p and ToS/DSCP values in incoming packets; untrusted ports will set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured.

qos port *chassis/slot/port***[**-*port2***] trusted**

qos port *chassis/slot/port* **no trusted**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

Defaults

By default, all ports are untrusted.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **qos trust-ports** command to set the default trust mode for all QoS ports. The **qos port trusted** command may be used to override the default.
- The setting applies only to ports with incoming traffic.
- Use the **qos port default 802.1p** or **qos port default dscp** commands to specify that a value other than zero should be applied to the incoming packets. Note that this value is overridden if a policy exists that specifies a different 802.1p or ToS/DSCP value for such packets.

Examples

```
-> qos port 3/1 trusted
-> qos port 4/2 no trusted
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
qos trust-ports	Configures the global trust mode for QoS ports.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortTrusted
```

qos port maximum egress-bandwidth

Configures the maximum rate at which to send traffic on the specified QoS port.

qos port *chassis/slot/port***[**-*port2***] maximum egress-bandwidth** *bps***[k | m | g | t]**

qos port *chassis/slot/port***[**-*port2***] no maximum egress-bandwidth**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
*bps***[k | m | g | t]**	The maximum amount of bandwidth, in bits-per-second, for all traffic that egresses on the port. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m, 1g, 1t**).

Defaults

By default, the maximum bandwidth is the maximum allowed for the interface type on which the port resides.

parameter	default
k | m | g | t	**k**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to remove a configured maximum egress bandwidth value from a port.
- If the maximum egress bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number **10** is specified, **10K** is the maximum bandwidth value used. However, if **10G** is specified, the maximum bandwidth value applied is **10** gbps.
- The maximum egress bandwidth value cannot exceed the maximum bandwidth of the interface type associated with the port.
- Modifying the maximum egress bandwidth is most useful for low-bandwidth links.

Examples

```
-> qos port 3/1 maximum egress-bandwidth 1000
-> qos port 4/1-8 maximum egress-bandwidth 10m
-> qos port 3/1 no maximum egress-bandwidth
-> qos port 4/1-8 no maximum egress-bandwidth
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos port maximum ingress-bandwidth	Configures the rate at which traffic is received on a QoS port.
qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortMaximumBandwidth
   alaQoSPortMaximumBandwidthStatus
```

qos port maximum ingress-bandwidth

Configures the maximum rate at which traffic is received on a QoS port.

qos port *chassis/slot/port***[**-*port2***] maximum ingress-bandwidth** *bps***[k | m | g | t]**

qos port *chassis/slot/port***[**-*port2***] no maximum ingress-bandwidth**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
*bps***[k | m | g | t]**	The maximum amount of bandwidth, in bits-per-second, for all traffic that ingresses on the port. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m, 1g, 1t**).

Defaults

By default, the maximum bandwidth is the maximum allowed for the interface type on which the port resides.

parameter	default
k | m | g | t	**k**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to remove a configured maximum ingress bandwidth value from a port.
- If the maximum ingress bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number **10** is specified, **10K** is the maximum bandwidth value used. However, if **10G** is specified, the maximum bandwidth value applied is **10** gbps.
- The maximum ingress bandwidth value cannot exceed the maximum bandwidth of the interface type associated with the port.
- Modifying the maximum ingress bandwidth is most useful for low-bandwidth links.

Examples

```
-> qos port 3/1 maximum ingress-bandwidth 1000
-> qos port 4/1-8 maximum ingress-bandwidth 10m
-> qos port 3/1 no maximum ingress-bandwidth
-> qos port 4/1-8 no maximum ingress-bandwidth
```

Release History

Release 7.1.1; command introduced.

Related Commands

qos port maximum egress-bandwidth	Configures the rate at which traffic is sent on a QoS port.
qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortMaximumIngBandwidth
   alaQoSPortMaximumIngBandwidthStatus
```

qos port maximum depth

Configures the maximum queue depth or bucket size assigned to this action, in bytes, used for traffic metering. The queue depth or bucket size determines the amount of buffer allocated to each queue. When the queue depth or bucket size is reached, the switch starts dropping packets.

qos port *chassis/slot/port***[**-*port2***] maximum {ingress | egress}-depth** *bytes* **[k | m | g | t]**

qos port *chassis/slot/port***[**-*port2***] no maximum {ingress | egress}-depth**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports.
*bytes***[k | m | g | t]**	The maximum bucket size, in bytes. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m**).

Defaults

parameter	default
k | m | g | t	**k**
bytes	**0**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- This QoS port parameter is configured in conjunction with the maximum bandwidth parameters. When the bucket size is reached, the switch starts to drop packets.
- Use the **no** form of the command to remove the maximum depth setting from a port.
- If the maximum depth value is specified as an integer, without an abbreviated unit designation, the value is applied in Kbytes by default. For example, if the number **10** is specified, **10K** is the maximum depth value used. However, if **1M** is specified, the maximum depth value applied is 1 Mbyte.
- Modifying the maximum depth is most useful for low-bandwidth links.

Examples

```
-> qos port 3/1 maximum ingress-depth 100
-> qos port 4/1-8 maximum egress-depth 10m
-> qos port 3/1 no maximum ingress-depth
-> qos port 4/1-8 no maximum egress-depth
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortMaximumDefaultDepth
```

qos port default 802.1p

Configures the 802.1p value to be inserted in flows ingressing on an untrusted port.

qos port *chassis/slot/port***[**-*port2***]** **default 802.1p** *value*

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
value	The priority value to be set. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- By default untrusted ports will set the 802.1p bit to zero on incoming flows. Use this command to specify that a different 802.1p value should be applied to the flow.
- The default 802.1p value is not used if there is a matching QoS policy rule that sets the priority.
- Note that the 802.1p bit for tagged packets received on untrusted ports is set with the default 802.1p value, which is configured using the **qos port default 802.1p** command. If the packet is untagged, however, then the DSCP bit is set with the default DSCP value, which is configured using the **qos port default dscp** command.

Examples

```
-> qos port 3/1 default 802.1p 5
-> qos port 4/1-8 default 802.1p 7
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDefault8021p
```

qos port default dscp

Configures the ToS/DSCP value to be inserted in flows ingressing on an untrusted port.

qos port *chassis/slot/port***[**-*port2***]** **default dscp** *value*

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
value	The ToS/DSCP value. The range is 0–63.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The value configured by this command sets the upper byte (precedence) and therefore configures the ToS/DSCP value for the port.
- The default DSCP value is not used if there is a matching QoS policy rule that sets the priority.
- Note that on the 802.1p bit for tagged packets received on untrusted ports is set with the default 802.1p value, which is configured using the **qos port default 802.1p** command. If the packet is untagged, however, then the DSCP bit is set with the default DSCP value, which is configured using the **qos port default dscp** command.

Examples

```
-> qos port 3/1 default dscp 63
-> qos port 4/1-8 default dscp 33
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDefaultDSCP
```

qos port default classification

Specifies the default egress priority value to use for IP traffic ingressing on trusted ports.

qos port *chassis/slot/port***[**-*port2***] default classification {tos | 802.1p | dscp}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
tos	Specifies that the ToS value of the flow will be used to prioritize flows coming in on the port.
802.1p	Specifies that the 802.1p value of the flow will be used to prioritize flows coming in on the port.
dscp	Specifies that the DSCP value of the flow will be used to prioritize flows coming in on the port.

Defaults

parameter	default
tos | 802.1p | dscp	dscp

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The egress priority assigned to an IP packet received on a trusted port is based on the DSCP value of the packet unless 802.1p is specified using this command.
- The default classification priority is not used if there is a matching QoS policy rule that sets the egress priority value.
- This command does not affect Layer 2 traffic, which is always classified with 802.1p.
- In some network situations, some IP traffic may be dropped before any QoS rules can take effect for the traffic.

Examples

```
-> qos port 8/24 default classification dscp
-> qos port 4/1-8 default classification dscp
-> qos port 7/1 default classification 802.1p
-> qos port 5/1-8 default classification 802.1p
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDefaultClassification
```

qos port dei

Configures the Drop Eligible Indicator (DEI) bit mapping and marking setting for the specified QoS port. The DEI setting applies to packets marked yellow (non-conforming) as the result of Tri-Color Marking (TCM) or other rate limiting mechanisms.

qos port *chassis/slot/port* **dei {ingress | egress}**

qos port *chassis/slot/port* **no dei {ingress | egress}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (1/5).
ingress	Maps the DEI/CFI bit to yellow (non-conforming) if this bit is set for ingress traffic. *DEI mapping is not supported on the OmniSwitch 6465.*
egress	Marks the DEI/CFI bit for egress packets if the packets were marked yellow as a result of the rate limiting process.

Defaults

By default, no DEI/CFI bit mapping or marking is done.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the DEI bit mapping (ingress) or marking (egress) configuration for the specified port
- Use the **qos dei** command to set the global DEI bit mapping and marking configuration for all QoS switch ports. Note that the port-level setting takes precedence over the global DEI setting.
- Packets marked yellow by rate limiting are still transmitted when there is no congestion on the egress port queues. Setting the DEI bit for yellow egress packets (**qos port dei egress**) ensures that an upstream switch is made aware that the packet was marked yellow.
- When a switch receives a yellow packet with the DEI bit set and ingress DEI bit mapping is enabled (**qos port dei ingress**), the packet is mapped to an internal drop precedence or yellow color marking for the switch.
- DEI bit mapping is not supported on the OmniSwitch 6465. As a result, packets are processed as follows on that switch:
  - When packets are received on a trusted port, the DEI bit is retained only if the packets were not subject to a meter. If the port is untrusted, however, the DEI bit is always reset.
  - When a meter is set and DEI egress is configured on a trusted port, the DEI bit is reset to 0 for green packets. Yellow–red packets egress with the DEI bit set to 1.

Examples

```
-> qos port 1/10 dei ingress
-> qos port 1/20 dei egress
-> qos port 1/10 no dei ingress
-> qos port 1/20 no dei egress
```

Release History

Release 7.2.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos dei	Configures the global Drop Eligible Indicator (DEI) bit mapping and marking setting for all QoS ports.
policy action cir	Configures a Tri-Color Marking policy action.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
   alaQoSPortDEIMapping
   alaQoSPortDEIMarking
```

qos qsp import

Imports a predefined QSet profile (QSP) to a new or previous custom profile.

qos qsp {*qsp_id* **|** *qsp_name***} import qsp {***import_qsp_id* **|** *import_qsp_name***}**

no qos qsp {*qsp_id* **|** *qsp_name***}**

Syntax Definitions

qsp_id	A QSet custom profile ID. The valid custom profile ID range is 6–16.
qsp_name	The QSet profile name.
import_qsp_id	The ID of the QSet profile to import (1 or 5).
import_dcp_name	The name of the QSet profile to import (QSP-1 or QSP-5).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 9900

Usage Guidelines

- The new QSet profile must be unique and not contain the same name and ID of an existing QSet profile.
- Use the **no** form of the command to remove an existing custom QSet profile from the switch configuration.
- The predefined QSet profiles 1 and 5 cannot be removed from the switch configuration.
- A custom profile can be assigned to any port or link aggregate, but not to a VFL link.
- A custom profile attached to a port cannot be removed from the switch configuration. In this case, the profile must be disassociated from the port before being removed.

Examples

```
-> qos qsp 12 import qsp 1
-> qos qsp qsp-16 import qsp 5
-> no qsp 12
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

qos qsi qsp	Configures the QSet profile association for the QSet instance.
show qos qsp	Displays the QSet profile attributes.

MIB Objects

```
alaVfcQsetProfileTable
   alaVfcQSPId
   alaVfcQSPName
   alaVfcQSPTemplateId
   alaVfcQSPTemplateName
   alaVfcQSPRowStatus
```

qos qsp qp

Modifies the Peak Information Rate (PIR), WFQ weight, and WFQ scheduler mode attributes for an individual queue profile (QP) associated with a custom QSet profile (QSP).

qos qsp {*qsp_id* **|** *qsp_name***} qp** *qp_id* **{pir** *%* | **weight** *weight* **| scheduler {sp | wrr | wrr2}}**

Syntax Definitions

qsp_id	A QSet custom profile ID. The valid custom profile ID range is 6–16.
qsp_name	The QSet custom profile name.
qp_id	The queue profile number in the QSet custom profile.
%	The PIR rate limit to apply to queue traffic.
weight	The queue weight that is used to determine the amount of shared bandwidth allocated for queue traffic. The valid range is 0–127.
sp	Selects the Strict Priority scheduler.
wrr	Selects the Weighted Round Robin scheduler.
wrr2	Selects a second Weighted Round Robin scheduler that is available on the OmniSwitch 9900.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 9900

Usage Guidelines

- The queue weight value is only used when WRR is the scheduler for the queue.
- The **pir**, **weight**, and **scheduler** attributes are only configurable for individual queues that are associated with a custom QSet profile.
- When a custom profile is modified, the changes are applied to all ports that are associated with that custom profile. To apply specific changes to a single port (QSet instance), import a custom or default profile into a new custom profile, make the necessary changes, then apply the new custom profile to the port.

Examples

```
-> qos qsp 6 qp 1 scheduler wrr weight 2 pir 100
-> qos qsp 6 qp 2 scheduler wrr weight 1 pir 100
-> qos qsp 6 qp 3 scheduler wrr weight 3 pir 100
-> qos qsp 6 qp 4 scheduler wrr weight 4 pir 100
-> qos qsp 6 qp 5 scheduler wrr weight 2 pir 100
-> qos qsp 6 qp 6 scheduler sp pir 50
-> qos qsp 6 qp 7 scheduler wrr2 weight 2 pir 100
-> qos qsp 6 qp 8 scheduler wrr2 weight 2 pir 100
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

qos qsp import	Creates a custom QSet profile.
show qos qsp	Displays the QSet profile attributes.

MIB Objects

```
alaVfcQProfileTable
   alaVfcQPQSPId
   alaVfcQPQSPName
   alaVfcQPQId
   alaVfcQPPIRBandwidthLimitType
   alaVfcQPPIRBandwidthLimitValue
   alaVfcQPWfqWeight
   alaVfcQPWfqMode
```

qos qsi qsp

Configures the QSet profile (QSP) association for the specified QSet instance (QSI). A QSI is a set of eight queues that is automatically associated with each port, link aggregate, and virtual fabric link (VFL).

qos qsi {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***] | vf-link** *vfl_id***} qsp {***qsp_id* **|** *qsp_name***}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number to associate with the QSet. Use a hyphen to specify a range of ports (3/1-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID to associate with the QSet. Use a hyphen to specify a range of IDs (10-20).
vfl_id	The VFL link ID (1/0). *This parameter option is supported only on the OmniSwitch 6860 and OmniSwitch 6865.*
qsp_id	An existing QSet profile (QSP) ID number to assign to this instance. • OmniSwitch 6465, OmniSwitch 6560, and OmniSwitch 9900 support predefined QSP IDs 1 and 5; profiles 2, 3, and 4 are not supported. Custom profiles QSP IDs 6 through 16 are supported. • OmniSwitch 6900-C32 and OmniSwitch 6900-V72 support predefined QSP ID 1; custom profiles are not supported. • OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 6900 support predefined QSP IDs 1, 2, 3, and 4; custom profiles are not supported.
qsp_name	An existing QSet profile name (for example, qsp-1) to assign to this instance.

Defaults

By default, QSP 1 is assigned to each QSet instance.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- There is only one QSI for each port, link aggregate, and VFL and only one QSP associated with each QSI.
- A QSI hierarchy exists consisting of parent/child relationships. For example, all member ports of a link aggregate will import the QSI/QSP settings of the parent link aggregate. When a member port moves out of the link aggregate, the QSI/QSP settings for that port are reset to the default settings.
- The number of children supported for a LAG ID is 8.
- On an OmniSwitch 6860 or OmniSwitch 6865, changing the QSP assignment for one VFL instance automatically changes the QSP assignment for all other VFL instances to the same QSP. For example, if QSP 2 is assigned to VFL 1/0, then the QSP assignment for VFL 2/0 is also changed to QSP 2. It is not necessary to configure the QSP assignment separately for each VFL on the switch.

Examples

```
-> qos qsi port 1/2 qsp 2
-> qos qsi port 2/1-10 qsp 3
-> qos qsi slot 3 qsp 4
-> qos qsi linkagg 10 qsp 2

The following command examples show that when the QSP assignment for VFL 1 is
changed to QSP 2, the QSP for VFL 2 is automatically changed as well:

-> qos qsi vf-link 1/0 qsp 2
WARNING: configuration change applied to all VFLs in the system

-> show qos qsi vf-link 1/0 summary
Legends: * indicates port is misconfigured.

           Profile
Port       #   Name         Mode Parent
----------+---+------------+----+------
vfl-1/0    2   qsp-2        NDCB vfl-1/0

-> show qos qsi vf-link 2/0 summary
Legends: * indicates port is misconfigured.

           Profile
Port       #   Name         Mode Parent
----------+---+------------+----+------
vfl-2/0    2   qsp-2        NDCB vfl-2/0
```

Release History

Release 7.2.1.R02; command introduced.
Release 8.3.1; **vf-link** parameter added.

Related Commands

qos qsp import	Imports a predefined QSet profile (QSP) to a new or previous custom profile.
qos qsi stats	Configures statistics collection for the QSet instance.
show qos qsi	Displays the QSet instance configuration.
show qos qsp	Displays the QSet profile attributes.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsetInstanceTable
   alaVfcQsetId
   alaVfcQsetQSPId
   alaVfcQsetQSPName
```

qos qsp system-default

Changes the default QSet profile (QSP) that is assigned to each port, link aggregate ID, and virtual fabric link (VFL).

qos qsp system-default {*qsp_id* **|** *qsp_name***}**

Syntax Definitions

qsp_id	An existing QSet profile (QSP) ID number to use as the default QSP. The valid range is 1–4.
qsp_name	An existing QSet profile name (qsp-1, qsp-2, qsp-3, qsp-4) to use as the default QSP.

Defaults

By default, QSP 1 is assigned to each QSet instance.

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

- When this command is used, the specified QSP is assigned to all ports, link aggregates, and VFLs on the switch.
- Changing the system default profile is only allowed when the switch is running in the non-Data Center Bridging (NDCB) mode. This mode is active by default when there is no OmniSwitch Data Center software license installed on the switch.
- A QSP assigned through the **qos qsi qsp** command overrides the system default QSP assignment. For example, if the system default QSP is set to 1 and the **qos qsi qsp** command is used to change the QSP to 2 on port 1/1/20, the QSP 2 settings are applied to port 1/1/20.

Examples

```
-> qos qsp system-default 2
-> qos qsp system-default qsp-4
```

Release History

Release 8.3.1; command introduced.

Related Commands

qos qsi qsp	Configures the QSet profile association for the QSet instance.
show qos qsp system-default	Displays the name and ID of the default QSP for the switch.

MIB Objects

```
alcatelIND1VfcMIB
   alaVfcSystemDefaultQsetQSPName
   alaVfcSystemDefaultQsetQSPId
```

qos qsi stats

Configures the administrative status and interval for statistics collection for the specified QSet instance (QSI). A QSI is a set of eight queues that is automatically associated with each port and link aggregate (LAG) ID.

qos qsi {port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} stats {admin-state {enable | disable} | interval** *interval_time***}]}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number to associate with the QSet. Use a hyphen to specify a range of ports (3/1-10).
*agg_id***[-***agg_id2***]**	The link aggregate ID to associate with the QSet. Use a hyphen to specify a range of IDs (10-20).
enable	Enables statistics collection for the instance.
disable	Disables statistics collection for the instance.
interval_time	The time interval for statistics gathering. The valid range is 10–300 seconds.

Defaults

By default, statistics collection is disabled and the time interval is set to 10 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- There is only one QSI per port or LAG ID and only one QSet profile (QSP) or DCB profile (DCP) associated with the QSI.
- Changing the statistics collection status for a QSI only changes the status for the port or link aggregate to which the QSI is associated.

Examples

```
-> qos qsi port 1/2 stats admin-state enable
-> qos qsi port 1/2 stats interval 30
-> qos qsi port 2/1-10 stats admin-state enable
-> qos qsi linkagg 10 stats admin-state enable interval 120
```

Release History

Release 7.2.1.R02; command introduced.

Related Commands

qos qsi qsp	Configures the QSet profile association for the QSet instance.
show qos qsi	Displays the QSet instance configuration.
show qos qsi stats	Displays statistics for one or more QSet instances.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsetInstanceTable
   alaVfcQsetQSPId
   alaVfcQsetQSPName
   alaVfcQsetStatsAdmin
   alaVfcQsetStatsInterval
```

show qos port

Displays information about all QoS ports or a particular port.

show qos port [*chassis/slot/port***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Information for all ports is displayed unless a particular port is specified.
- Use the **qos port** command to configure port parameters.
- For ports that are trusted (**Yes** displays in the Trust field), the Trust field includes one of the following characters:

character	definition
+	Indicates that the port is manually configured as trusted through the **qos port trusted** command; the port setting takes precedence over the global trust setting configured through the **qos trust-ports** command.
*	Indicates that the port is automatically trusted regardless of the global setting set through the **qos trust-ports** command. (Applies to mobile ports and ports configured for 802.1Q.)

Examples

```
-> show qos port
Slot/              Default    Default                Bandwidth       DEI
Port  Active Trust P/DSCP Classification  Physical Ingress Egress  Map/Mark    Type
-----+------+-----+------+--------------+--------+-------+-------+---------+-------------
 1/1    No     No  0/ 0           DSCP          0K       -       -   No / No   ethernet
 1/2   Yes     No  0/ 0           DSCP       1.00G       -       -   No / No   ethernet-1G
 1/3    No     No  0/ 0           DSCP          0K       -       -   No / No   ethernet
 1/4    No     No  0/ 0           DSCP          0K       -       -   No / No   ethernet
 1/5    No     No  0/ 0           DSCP          0K       -       -   No / No   ethernet
 1/6    No     No  0/ 0           DSCP          0K       -       -   No / No   ethernet
 1/7    No     No  0/ 0           DSCP          0K       -       -   No / No   ethernet
 1/8    No     No  0/ 0           DSCP          0K       -       -   No / No   ethernet
 1/9    No     No  0/ 0           DSCP          0K       -       -   No / No   ethernet
 1/10   No     No  0/ 0           DSCP          0K     50K       -   No / No   ethernet
 1/11   No   *Yes  0/ 0         *802.1P         0K       -       -   No / No   ethernet
 1/12   No   *Yes  0/ 0         *802.1P         0K       -       -   No / No   ethernet
```

```
-> show qos port 1/2
Slot/              Default    Default                Bandwidth       DEI
Port  Active Trust P/DSCP Classification  Physical Ingress Egress  Map/Mark    Type
-----+------+-----+------+---------------+--------+-------+-------+---------+-------------
 1/2   Yes     No  0/ 0           DSCP       1.00G       -       -   No / No   ethernet-1G
```

output definitions

Slot/Port	The slot and physical port number.
Active	Whether or not the port is sending/receiving QoS traffic.
Trust	Whether the port is trusted or not trusted. Configured through the **qos port trusted** command.
Default P	The default 802.1p setting for the port. Configured through the **qos port default 802.1p** command.
Default DSCP	The default ToS/DSCP setting for the port. Configured through the **qos port default dscp** command.
Default Classification	The default classification setting for the port (**802.1p, ToS,** or **DSCP**). Configured through the **qos port default classification** command.
Physical Bandwidth	The amount of physical bandwidth available on the port.
Ingress Bandwidth	The amount of ingress bandwidth configured for the port. Configured through the **qos port maximum ingress-bandwidth** command.
Egress Bandwidth	The amount of egress bandwidth configured for the port. Configured through the **qos port maximum egress-bandwidth** command.
DEI Map/Mark	The Drop Eligible Indicator (DEI) bit mapping and marking setting for the port. Configured through the **qos port dei** command.
Type	The interface type, **ethernet** or **wan**.

Release History

Release 7.1.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.

MIB Objects

```
alcatelIND1VfcMIB
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortEnabled
   alaQoSPortDefault8021p
   alaQoSPortDefaultDSCP
   alaQoSPortMaximumDefaultBandwidth
   alaQoSPortDefaultClassification
```

show qos slice

Displays rule availability and usage information for QoS slices of QoS slots. A *slice* is a logical section of hardware and corresponds to particular ports on the interface.

show qos slice [*slot/slice***]**

Syntax Definitions

slot/slice	The slot number and slice for which you want to view information. The number of slices per module varies depending on the type of module.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Information for all slots/slices is displayed unless a particular slot/slice is requested.
- This command is useful for monitoring switch resources required for policy rules.
- On the following switch platforms, use the **show tcam utilization** command instead of the **show qos slice** command:
  - OmniSwitch 6465
  - OmniSwitch 6560
  - OmniSwitch 6900-V72, 6900-C32
  - OmniSwitch 9900

Examples

```
-> show qos slice
Slot/                    Ranges          Rules          Counters         Meters
Unit            Type Total/Free  CAM Total/Free      Total/Free      Total/Free
 1/1/(0)        IFP    24/24       0   256/252          256/252         256/256
                                   1   256/255          256/255         256/256
                                   2   256/256          256/256         256/256
                                   3   256/256          256/256         256/256
                                   4   256/256          256/256         256/256
                                   5   256/256          256/256         256/256
                                   6   256/256          256/256         256/256
                                   7   256/256          256/256         256/256
                                   8   256/256          256/256         256/256
                                   9   256/256          256/256         256/256
                                  10   256/256          256/256         256/256
                                  11   256/256          256/256         256/256
                                  12   256/256          256/256         256/256
                                  13   256/256          256/256         256/256
                                  14   256/255          256/254         256/254
```

```
                                    15   256/255          256/256          256/256
1/1/(0)          EFP      0/0       0   256/256          256/256          256/256
                                    1   256/256          256/256          256/256
                                    2   256/256          256/256          256/256
                                    3   256/256          256/256          256/256
```

output definitions

Slot/Unit	The slot and slice number.
Type	The type of slice.
Ranges Total	The total number of TCP/UDP port ranges supported per slot/slice.
Ranges Free	The number of TCP/UDP port ranges that are still available for use.
CAM	The CAM number.
Rules Total	The total number of rules supported per CAM.
Rules Free	The number of rules that are still available for use. On startup, the switch uses 27 rules.
Counters Total	The total number of counters supported per CAM.
Counter Free	The number of counters that are still available for use.
Meters Total	The total number of meters supported per CAM.
Meters Free	The number of meters that are still available for use.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

N/A

show qos log

Displays the log of QoS events.

show qos log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display the current QoS log. To clear the log, use the **clear qos log** command.

Examples

```
-> show qos log
**QOS Log**
Insert rule 0
Rule index at 0
Insert rule 1
Rule index at 1
Insert rule 2
Rule index at 2
Enable rule r1 (1) 1,1
Enable rule r2 (0) 1,1
Enable rule yuba1 (2) 1,1
Verify rule r1(1)
Enable rule r1 (1) 1,1
Really enable r1
Update condition c1 for rule 1 (1)
Verify rule r2(1)
Enable rule r2 (0) 1,1
Really enable r2
Update condition c2 for rule 0 (1)
Verify rule yuba1(1)
Enable rule yuba1 (2) 1,1
Really enable yuba1
Update condition yubamac for rule 2 (1)
QoS Manager started TUE MAR 10 13:46:50 2002

Match rule 2 to 1
Match rule 2 to 2
Match rule 2 to 3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

clear qos log	Clears messages in the current QoS log.
qos log lines	Configures the number of lines in the QoS log.

MIB Objects

N/A

show qos config

Displays global information about the QoS configuration.

show qos config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to view the current global configuration for QoS. Use the **show qos statistics** command to view statistics about the QoS software in the switch.

Examples

```
-> show qos config
QoS Configuration
  Admin                         = enable,
  Switch Group                  = expanded,
  Trust ports                   = no,
  Phones                        = trusted,
  Log lines                     = 10240,
  Log level                     = 5,
  Log console                   = no,
  Forward log                   = no,
  Stats interval                = 60,
  User-port filter              = spoof,
  User-port shutdown            = none,
  Debug                         = info,
  DEI Mapping                   = Disabled,
  DEI Marking                   = Disabled,
  Pending changes               = none
```

output definitions

Admin	Whether or not QoS is enabled or disabled. Configured through the **qos** command.
Switch Group	Whether the expanded or compact method is used to populate the hardware routing table. Configured through the **qos switch-group** command.
Trust Ports	The default trusted mode for switch ports. Configured through the **qos trust-ports** command.

output definitions (continued)

Phones	Whether or not IP Phone traffic is automatically trusted or assigned a priority value. Configured through the **qos phones** command.
Log lines	The number of lines included in the QoS log. Configured through the **qos log lines** command.
Log level	The level of log detail. Configured through the **qos log level** command.
Log console	Whether or not log messages are sent to the console. Configured through the **qos log console** command.
Forward log	Whether or not logged events are sent to the policy server software in the switch in real time. Configured through the **qos forward log** command.
Stats interval	How often the switch polls network interfaces for statistics about QoS events. Configured through the **qos stats interval** command.
User-port filter	The type of traffic that is filtered on ports that are members of the UserPorts group. Configured through the **qos user-port** command.
User-port shutdown	The type of traffic that will trigger an administrative shutdown of the port if the port is a member of the UserPorts group. Configured through the **qos user-port** command.
Debug	The type of information that will be displayed in the QoS log. A value of **info** indicates the default debugging type.
DEI Mapping	The status (enabled or disabled) of Drop Eligible Indicator (DEI) bit mapping for ingress traffic. Configured through the **qos dei** command.
DEI Marking	The status (enabled or disabled) of DEI bit marking for egress traffic. Configured through the **qos dei** command.
Pending changes	QoS changes not yet applied to the configuration.

Release History

Release 7.1.1; command was introduced.

Related Commands

qos	Enables or disables QoS. This base command may be used with keyword options to configure QoS globally on the switch.
show qos statistics	Displays statistics about the QoS configuration.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigEnable
   alaQoSConfigSwitchGroup
   alaQosConfigTrustPorts
   alaQoSConfigAutoPhones
   alaQoSConfigLogLines
   alaQoSConfigLogLevel
   alaQoSConfigLogConsole
   alaQoSConfigStatsInterval
   alaQosConfigUserportFilter
   alaQosConfigUserportShutdown
   alaQosConfigDebug
   alaQoSConfigDEIMapping
   alaQoSConfigDEIMarking
```

show qos statistics

Displays statistics about the QoS configuration.

show qos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command displays statistics about the global QoS configuration. Use the **show qos config** command to display information about configurable global parameters.

Examples

```
-> show qos statistics
QoS stats
                          Events   Matches     Drops
  L2                   :         0         0         0
  L3 Inbound           :         0         0         0
  L3 Outbound          :         0         0         0
  IGMP Join            :         0         0         0
  Fragments            : 0
  Bad Fragments        : 0
  Unknown Fragments    : 0
  Sent NI messages     : 0
  Received NI messages : 85
  Failed NI messages   : 4
  Max PTree nodes      : 0
  Max PTree depth      : 0
  Spoofed Events       : 0
  NonSpoofed Events    : 0

Software resources
                      Applied                 Pending
           Table  CLI LDAP  Blt Total     CLI LDAP  Blt Total     Max
           rules    0    0    0     0       0    0    0     0    8192
         actions    0    0    0     0       0    0    0     0    8192
      conditions    0    0    0     0       0    0    0     0    8192
        services    0    0    0     0       0    0    0     0     256
  service groups    0    0    0     0       0    0    0     0    1024
  network groups    0    0    1     1       0    0    1     1    1024
     port groups    1    0    0     1       1    0    0     1    1024
      mac groups    0    0    0     0       0    0    0     0    1024
      map groups    0    0    0     0       0    0    0     0    1024
```

```
validity periods    0    0    0     0       0    0    0     0      64

Hardware resources          TCAM                Ranges
   Slot Slice Unit   Used  Free   Max    Used  Free   Max
   0/ 1     0    0      1  1023  1024       0    32    32
```

output definitions

Events	The number of Layer 2 or Layer 3 flows transmitted on the switch.
Matches	The number of Layer 2 or Layer 3 flows that match policies.
Drops	The number of Layer 2 or Layer 3 flows that were dropped.
L2	The number of Layer 2 events, matches, and drops.
L3 Ingress	The number of Layer 3 ingress events, matches, and drops.
L3 Egress	The number of Layer 3 egress events, matches, and drops
IGMP join	The number of multicast events, matches, and drops.
Fragments	The number of fragments dropped.
Bad Fragments	The number of fragments received with an offset of 1.
Unknown Fragments	The number of out-of-order fragments received.
Sent NI messages	The number of messages sent to network interfaces.
Received NI messages	The number of messages received by network interfaces.
Failed NI messages	The number of failed message attempts to network interfaces.
Load balanced flows	The number of Server Load Balance flow entries.
Reflexive flows	The number of reflexive flows.
Reflexive correction	The number of reflexive flow corrections.
Flow lookups	The number of flow table lookups.
Flow hits	The number of flow table lookup hits.
Max PTree nodes	The highest number of nodes in the classifier tree.
Max Ptree depth	The length of the longest path in the classifier tree.
Spoofed Events	The number of spoofed events.
Nonspoofed Events	The number of non-spoofed events.
DropServices	The number of TCP/UDP flows dropped.

Release History

Release 7.1.1; command was introduced.

Related Commands

qos stats reset	Resets QoS statistic counters to zero.

MIB Objects

```
alaQoSStats
   alaQoSStatsL2Events
   alaQoSStatsL2matches
   alaQoSStatsL2Drops
   alaQoSStatsL3IngressEvents
   alaQoSStatsL3IngressMatches
   alaQoSStatsL3IngressDrops
   alaQoSStatsL3EgressEvents
   alaQoSStatsL3EgressMatches
   alaQoSStatsL3EgressDrops
   alaQoSStatsFragments
   alaQoSStatsBadFragments
   alaQoSStatsUnknownFragments
   alaQoSStatsSpoofedEvents
   alaQoSStatsNonspoofedEvents
```

show qos qsi summary

Displays a list of switch ports showing the QoS or DCB profile assigned to each port.

show qos qsi [port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]] summary**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

By default, a summary of all ports is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enter a port or link aggregate ID with this command to display information for a specific port or link aggregate.

Examples

```
-> show qos qsi summary
Legends: * indicates port is misconfigured.

           Profile
Port       #   Name         Mode Parent
----------+---+------------+----+------
1/1/1      1   qsp-1        NDCB 1/1/1
1/1/2      1   qsp-1        NDCB 1/1/2
1/1/3      1   qsp-1        NDCB 1/1/3
1/1/4      1   qsp-1        NDCB 1/1/4
1/1/5      7   qsp-7        NDCB 1/1/5
1/1/6      1   qsp-1        NDCB 1/1/6

-> show qos qsi port 1/1-5 summary
Legends: * indicates port is misconfigured.

           Profile
Port       #   Name         Mode Parent
----------+---+------------+----+------
1/1/1      1   qsp-1        NDCB 1/1/1
1/1/2      1   qsp-1        NDCB 1/1/2
1/1/3      1   qsp-1        NDCB 1/1/3
1/1/4      1   qsp-1        NDCB 1/1/4
1/1/5      7   qsp-7        NDCB 1/1/5
```

output definitions

Port	Configured DCB ports.
Profile #	Identifies the DCB profile assigned to the port.
Profile Name	Name of the DCB profile assigned to the port.
Mode	Indicates if the port is DCB or NDCB.
Parent	Lists the parent of the port.

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsi dcb dcbx	Displays the configured ports in the system and the related DCBX information.
qos qsi qsp dcb	Assigns a DCB profile to a port or link aggregate.

MIB Objects

```
alaVfcQsetInstanceTable
   alaVfcQsetId
   alaVfcQsetQSPId
   alaVfcQsetQSPName
   alaDcbxPortInstanceTable
   alaVfcQsapParent
```

show qos qsp

Displays the QSet profile (QSP) configuration for the switch.

show qos qsp [*qsp_id* **|** *qsp_name***] [brief | detail [port** *chassis/slot/port***[-***port2***]] | linkagg** *agg_id***[-***agg_id2***]]]**

Syntax Definitions

qsp_id	A QSet profile (QSP) ID number. • OmniSwitch 6465, OmniSwitch 6560, and OmniSwitch 9900 support predefined QSP IDs 1 and 5; profiles 2, 3, and 4 are not supported. QSP IDs 6 through 16 refer to custom profiles that are also supported. • OmniSwitch 6900-C32 and OmniSwitch 6900-V72 support predefined QSP ID 1; custom profiles are not supported. • OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 6900 support predefined QSP IDs 1, 2, 3, and 4; custom profiles are not supported.
qsp_name	The name of a QSP profile.
brief	Displays a summary of the QSP configuration.
detail	Displays QSP configuration details for a specific profile, port, slot, or link aggregate.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[-***agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

By default, displays the configuration for all of the QSet profiles.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the *qsp_id* or the *qsp_name* parameter to display information for a specific profile.
- Use the **detail** parameter in combination with the **port** *slot/port* and **linkagg** *agg_id* parameters to display profile information associated with specific ports or link aggregates.
- Configuring a QSP assignment for a virtual fabric link (VFL) is supported only on the OmniSwitch 6860 and OmniSwitch 6865.

Examples

```
-> show qos qsp 1
QSP  1 (qsp-1)
  #Ports:  107, #Queues:  8, BW (%): 100,
  WRP:  1, Name:        wrp-1
  Scheduler: Qspec, Type: Sta,
  Template: 1, Name:        qsp-1
    QP  1
      Qtype: SP7,
      WRP:  1, Name:        wrp-1
      CIR (%):   0, PIR (%): 100,
      WFQ-Mode: WERR, WFQ-Weight:   1
    QP  2
      Qtype: SP6,
      WRP:  1, Name:        wrp-1
      CIR (%):   0, PIR (%): 100,
      WFQ-Mode: WERR, WFQ-Weight:   1
    QP  3
      Qtype: SP5,
      WRP:  1, Name:        wrp-1
      CIR (%):   0, PIR (%): 100,
      WFQ-Mode: WERR, WFQ-Weight:   1
    QP  4
      Qtype: SP4,
      WRP:  1, Name:        wrp-1
      CIR (%):   0, PIR (%): 100,
      WFQ-Mode: WERR, WFQ-Weight:   1
    QP  5
      Qtype: SP3,
      WRP:  1, Name:        wrp-1
      CIR (%):   0, PIR (%): 100,
      WFQ-Mode: WERR, WFQ-Weight:   1
    QP  6
      Qtype: SP2,
      WRP:  1, Name:        wrp-1
      CIR (%):   0, PIR (%): 100,
      WFQ-Mode: WERR, WFQ-Weight:   1
    QP  7
      Qtype: SP1,
      WRP:  1, Name:        wrp-1
      CIR (%):   0, PIR (%): 100,
      WFQ-Mode: WERR, WFQ-Weight:   1
    QP  8
      Qtype: SP0,
      WRP:  1, Name:        wrp-1
      CIR (%):   0, PIR (%): 100,
      WFQ-Mode: WERR, WFQ-Weight:   1
```

output definitions

QSP	The QSet profile (QSP) ID number and name.
#Ports	The number of ports to which this profile is attached.
#Queues	The number of queues associated with this QSet. Currently there are eight queues for each QSet.
BW%	The bandwidth percentage for the QSet. The bandwidth is shared between all the queues.

output definitions (continued)

WRP	*Not supported in this release.*
Name	*Not supported in this release.*
Scheduler	The type of scheduler, such as queue specific priority (Qspec) or strict priority.
Type	Whether the QSP is static or dynamic. Currently there are predefined, static profiles on each switch. User-configured, dynamic profiles are only supported on the OmniSwitch 6465, OmniSwitch 6560, and OmniSwitch 9900.
QP 1...8	The queue profile configuration for each QSet queue. The configuration for each of the individual queue profiles is defined by the QSP in use. For example, QSP 1 applies a different queue configuration than QSP 2, 3, or 4.

```
-> show qos qsp brief
Profile  Name          #Ports  #Queues  BW(%)  Type      Base Profile
--------+-------------+-------+--------+------+---------+-------------
1        qsp-1         58      8        100    Static    qsp-1
5        qsp-5         0       8        100    Static    qsp-5
6        qsp-6         0       8        100    Dynamic   qsp-5
```

output definitions

Profile	The QSet profile (QSP) ID number.
Name	The QSP name.
#Ports	The number of ports to which this profile is attached.
#Queues	The number of queues associated with this QSet. Currently there are eight queues for each QSet.
BW%	The bandwidth percentage for the QSet. The bandwidth is shared between all the queues.
Type	Whether the QSP is static or dynamic. Currently there are predefined, static profiles on each switch. User-configured, dynamic profiles are only supported on the OmniSwitch 6465, OmniSwitch 6560, and OmniSwitch 9900.
Base Profile	The profile on which the QSP is based. The profile number will differ for user-configured profiles.

```
-> show qos qsp detail

Legends: T (Type): S = Static, D = Dynamic

QSAP       QSAP                              QSAP           BW (%) BW (%)
Port       Type dQSI            ID Name       Parent         Admin  Oper      T
----------+----+--------------+--+----------+--------------+------+---------+-
1/1/1      Phy  Port 1/1/1      1  qsp-1      Port 1/1/1     100    100       S
1/1/2      Phy  Port 1/1/2      1  qsp-1      Port 1/1/2     100    100       S
1/1/3      Phy  Port 1/1/3      1  qsp-1      Port 1/1/3     100    100       S
1/1/4      Phy  Port 1/1/4      1  qsp-1      Port 1/1/4     100    100       S
1/1/5      Phy  Port 1/1/5      1  qsp-1      Port 1/1/5     100    100       S
1/1/6      Phy  Port 1/1/6      1  qsp-1      Port 1/1/6     100    100       S
1/1/7      Phy  Port 1/1/7      1  qsp-1      Port 1/1/7     100    100       S
```

```
1/1/8      Phy  Port 1/1/8     1  qsp-1      Port 1/1/8     100    100       S
1/1/9      Phy  Port 1/1/9     1  qsp-1      Port 1/1/9     100    100       S
1/1/10     Phy  Port 1/1/10    1  qsp-1      VFL 1/0        100    100       S
1/1/11     Phy  Port 1/1/11    1  qsp-1      Port 1/1/11    100    100       S
1/1/12     Phy  Port 1/1/12    1  qsp-1      Port 1/1/12    100    100       S
.
.
.
2/1/27     Phy  Port 2/1/27    1  qsp-1      Port 2/1/27    100    100       S
2/1/28     Phy  Port 2/1/28    1  qsp-1      Port 2/1/28    100    100       S
2/1/29     Phy  Port 2/1/29    2  qsp-2      VFL 2/0        100    100       S
2/1/30     Phy  Port 2/1/30    1  qsp-1      Port 2/1/30    100    100       S
10         Log  Linkagg 10     1  qsp-1      Linkagg 10     100    100       S
vfl-1/0    Log  VFL 1/0        2  qsp-2      VFL 1/0        100    100       S
vfl-2/0    Log  VFL 2/0        2  qsp-2      VFL 2/0        100    100       S

-> show qos qsp detail port 1/1/12

Legends: T (Type): S = Static, D = Dynamic

QSAP       QSAP                              QSAP           BW (%) BW (%)
Port       Type dQSI           ID Name       Parent         Admin  Oper      T
-----------+----+--------------+--+----------+--------------+------+---------+-
1/1/12     Phy  Port 1/1/12    1  qsp-1      Port 1/1/12    100    100       S
```

output definitions

QSAP Port	The port number, link aggregate ID, or virtual fabric link (VFL) ID for the QSet attachment point (QSAP). A QSAP is a logical entity generated internally by the switch to identify the association between a QSet instance and a port, link aggregate, and VFL. The QSAP is not configurable at this time.
QSAP Type	The type of QSAP port; Phy = physical (slot/port), Log = logical (linkagg ID or VFL ID).
dQSI	The default QSet instance (dQSI) ID number. This number is generated internally by the switch to identify the QSI that is automatically assigned to each port, link aggregate, and VFL.
ID	The QSet profile (QSP) ID number.
Name	The QSP name.
QSAP Parent	The QSAP parent ID number. If the parent ID is different than the QSAP ID, then the port is a member of a link aggregate or a VFL.
BW (%) Admin	The administrative bandwidth percentage for the QSet. The administrative percentage is not configurable at this time.
BW (%) Oper	The operational percentage of bandwidth as determined by the port speed. For a link aggregate, this value is the sum of the operational bandwidth percentages for the member ports.
Type	Whether the QSP is static or dynamic. Currently there are predefined, static profiles on each switch. User-configured, dynamic profiles are only supported on the OmniSwitch 6465, OmniSwitch 6560, and OmniSwitch 9900.

Release History

Release 7.2.1; command was introduced.

Related Commands

qos qsi qsp	Changes the QSet profile association for a QSet instance.
show qos qsi	Displays the QSet instance configuration.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsetProfileTable
   alaVfcQSPId
   alaVfcQSPName
   alaVfcQSPBandwidthLimitValue
   alaVfcQSPQueueCount
   alaVfcQSPSchedulingMethod
   alaVfcQSPStatsAdmin
   alaVfcQSPAttachmentCount
```

show qos wrp

Displays the Weighted Random Early Detection (WRED) profile (WRP) configuration for the switch.

show qos wrp [*wrp_id* **|** *wrp_name***] [detail [port** *chassis/slot/port***[-***port2***]] | slot** *slot* **| linkagg** *agg_id***[-***agg_id2***]]]**

Syntax Definitions

wrp_id	A WRED profile (WRP) ID number. The valid range is 1.
wrp_name	A WRED profile name.
detail	Displays WRED profile configuration details for a port, slot, or link aggregate.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number of a non-DCB (Data Center Bridging) port. Use a hyphen to specify a range of ports (1/5-10).
slot	A slot number. Displays information for all non-DCB ports on the slot.
*agg_id***[-***agg_id2***]**	The link aggregate ID for a non-DCB aggregate. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is not supported on OmniSwitch 6900 DCB ports.
- Use the *wrp_id* or the *wrp_name* parameter to display information for a specific profile.
- Use the **detail** parameter to display additional profile information, such as the profile configuration associated with queues and ports.
- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to display profile information associated with specific ports or link aggregates. These parameters are used in combination with the **detail** parameter.

Examples

```
-> show qos wrp
WRP  1 (wrp-1)
  #Ports:  480, MTU:  1540
    Red
      Min-Th:  10, Max-Th:  50, Max-Pb:  36, Gain:  9
    Yellow
      Min-Th:  50, Max-Th:  90, Max-Pb:  30, Gain:  9
    Green
```

```
      Min-Th:  90, Max-Th: 100, Max-Pb:  24, Gain:  9
```

output definitions

WRP	The WRED profile (WRP) ID number and name.
#Ports	The number of ports to which this profile is attached.
MTU	The MTU size.
Min-Th	The minimum queue threshold percentage for red, green, and yellow packets.
Max-Th	The maximum queue threshold percentage for red, green, and yellow packets.
Max-Pb	The maximum drop probability percentage for red, green, and yellow packets.
Gain	The gain value to smooth out the queue (1–15).

```
-> show qos wrp 1 detail port 2/4
Port 2/4
  QSAP:    Port 2/4, Parent:    Port 2/4,
  WRP:  1, Name:        wrp-1, Admin: Dis
    QSI    Port 2/4
      QSP:  1, Name:        qsp-1, Admin: Ena
        QI  1
          WRP:  1, Name:        wrp-1, Admin: Dis
        QI  2
          WRP:  1, Name:        wrp-1, Admin: Dis
        QI  3
          WRP:  1, Name:        wrp-1, Admin: Dis
        QI  4
          WRP:  1, Name:        wrp-1, Admin: Dis
        QI  5
          WRP:  1, Name:        wrp-1, Admin: Dis
        QI  6
          WRP:  1, Name:        wrp-1, Admin: Dis
        QI  7
          WRP:  1, Name:        wrp-1, Admin: Dis
        QI  8
          WRP:  1, Name:        wrp-1, Admin: Dis
```

output definitions

Port	The physical slot and port number (or link aggregate ID for a logical port).
QSAP	The QSet attachment point (QSAP). This is a logical entity used internally by the switch to identify the association between a QSet instance and a port or link aggregate. The QSAP is not configurable at this time.
Parent	The QSAP ID for the parent QSAP, if any.
WRP Name Admin	The WRED profile (WRP) ID number, name, and administrative status.
QSI	The switch port associated with the QSet instance (QSI).
QSP Name Admin	The QSet profile (QSP) ID number, name, and administrative status.
QI 1...8	The WRP information for each of the QSet queues.

Release History

Release 7.2.1; command was introduced.

Related Commands

qos qsi qsp	Changes the QSet profile association for a QSet instance.
show qos qsi	Displays the QSet instance configuration.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcWREDProfileTable
   alaVfcWRPId
   alaVfcWRPAdminState
   alaVfcWRPName
   alaVfcWRPGreenMinThreshold
   alaVfcWRPGreenMaxThreshold
   alaVfcWRPGreenMaxDropProbability
   alaVfcWRPGreenGain
   alaVfcWRPYellowMinThreshold
   alaVfcWRPYellowMaxThreshold
   alaVfcWRPYellowMaxDropProbability
   alaVfcWRPYellowGain
   alaVfcWRPRedMinThreshold
   alaVfcWRPRedMaxThreshold
   alaVfcWRPRedMaxDropProbability
   alaVfcWRPRedGain
   alaVfcWRPMTU
   alaVfcWRPAttachmentCount
   alaVfcWRPLastChange
   alaVfcWRPRowStatus
```

show qos qsi

Displays the QSet instance (QSI) configuration for the switch. A QSI is a logical set of eight egress queues associated with each port, link aggregate (LAG) ID, and virtual fabric link (VFL).

show qos qsi [port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***] | vf-link** *vfl_id***] [detail | summary]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[-***agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
vfl_id	The VFL ID (1/0). *This parameter option is supported only on the OmniSwitch 6860 and OmniSwitch 6865.*
detail	Displays additional queue information for the instance.
summary	Displays summary information for the instance.

Defaults

By default, displays the entire QSI configuration for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **port** *slot/port*, **slot** *slot*, **linkagg** *agg_id,* and **vf-link** *vfl_id* parameters to display the QSI information associated with specific ports, link aggregates, or VFLs. These parameters can also be combined with the **detail** or **summary** parameters.

Examples

```
-> show qos qsi port 1/1/1
Port 1/1/1
  QSAP:  Port 1/1/1, Parent:  Port 1/1/1
    QSI  Port 1/1/1
      QSP:  1, Name:        qsp-1,
      WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
        Stats
          Admin: Dis, Oper: Dis, Interval:    60
        BW
          Admin (%): 100, Oper (%): 100

-> show qos qsi port 1/1/54
Port 1/1/54
  QSAP: Port 1/1/54, Parent:     VFL 1/0
    QSI Port 1/1/54
      QSP:  2, Name:        qsp-2,
      WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
```

```
        Stats
          Admin: Dis, Oper: Dis, Interval:    60
        BW
          Admin (%): 100, Oper (%): 100

-> show qos qsi vf-link 1/0
VFL 1/0
  QSAP:     VFL 1/0, Parent:     VFL 1/0
    QSI     VFL 1/0
      QSP:  1, Name:        qsp-1,
      WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
        Stats
          Admin: Dis, Oper: Dis, Interval:    60
        BW
          Admin (%): 100, Oper (%): 100

-> show qos qsi port 1/1/1 detail
Port 1/1/1
  QSAP:    Port 1/1/1, Parent:    Port 1/1/1
    QSI    Port 1/1/1
      QSP:  1, Name:        qsp-1,
      WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
        Stats
          Admin: Dis, Oper: Dis, Interval:    60
        BW
          Admin (%): 100, Oper (%): 100
        QI  1
          Qtype: SP7,
          WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
            CIR
              Admin (%):   0, Oper (%):   0
            PIR
              Admin (%): 100, Oper (%): 100
        QI  2
          Qtype: SP6,
          WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
            CIR
              Admin (%):   0, Oper (%):   0
            PIR
              Admin (%): 100, Oper (%): 100
        QI  3
          Qtype: SP5,
          WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
            CIR
              Admin (%):   0, Oper (%):   0
            PIR
              Admin (%): 100, Oper (%): 100
        QI  4
          Qtype: SP4,
          WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
            CIR
              Admin (%):   0, Oper (%):   0
            PIR
              Admin (%): 100, Oper (%): 100
        QI  5
          Qtype: SP3,
          WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
            CIR
              Admin (%):   0, Oper (%):   0
```

```
    PIR
      Admin (%): 100, Oper (%): 100
QI  6
  Qtype: SP2,
  WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
    CIR
      Admin (%):   0, Oper (%):   0
    PIR
      Admin (%): 100, Oper (%): 100
QI  7
  Qtype: SP1,
  WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
    CIR
      Admin (%):   0, Oper (%):   0
    PIR
      Admin (%): 100, Oper (%): 100
QI  8
  Qtype: SP0,
  WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
    CIR
      Admin (%):   0, Oper (%):   0
    PIR
      Admin (%): 100, Oper (%): 100
```

output definitions

QSAP	The port number, link aggregate ID, or virtual fabric link (VFL) ID for the QSet attachment point (QSAP). A QSAP is a logical entity generated internally by the switch to identify the association between a QSet instance and a port, link aggregate, and VFL. The QSAP is not configurable at this time.
Parent	The parent QSAP ID. If the parent ID is different than the QSAP ID, then the port is a member of a link aggregate or VFL.
QSI	The QSet instance (QSI) ID number, internally generated by the switch.
QSP, Name	The QSet profile (QSP) ID number and name associated with the QSI.
WRP, Name, Admin, Oper	*Not supported in this release.*
Stats, Admin, Oper, Interval	The QSI administrative status, operational status, and time interval for statistics collection.
BW Admin (%)	The administrative percentage of bandwidth (currently not user-configurable).
BW Oper (%)	The operational percentage of bandwidth as determined by the port speed. For a link aggregate, this value is the sum of the operational bandwidth percentages for the member ports.
QI 1–8	The queue scheduling and bandwidth configuration for each QSI queue. These values are determined by which one of the QSet profiles (QSP 1–4) is associated with the QSI.

```
-> show qos qsi port 1/1/20 summary
Legends: * indicates port is misconfigured.

           Profile
Port       #   Name         Mode Parent
----------+---+------------+----+------
1/1/20     1   qsp-1        NDCB 1/1/20

-> show qos qsi vf-link 1/0 summary
Legends: * indicates port is misconfigured.

           Profile
Port       #   Name         Mode Parent
----------+---+------------+----+------
vfl-1/0    2   qsp-2        NDCB vfl-1/0
```

output definitions

Port	The physical slot and port number (or link aggregate ID or VFL ID for a logical port).
Profile #, Name	The QSet profile (QSP) ID number and name associated with the QSI.
Mode	The QSI operating mode (**NDCB** or **DCB**). This mode determines whether Data Center Bridging (DCB) profiles or QSet profiles (non-DCB) are applied to the QSI instance. DCB and QSet profiles are mutually exclusive in that if the OmniSwitch Data Center software license is installed, only DCB profiles are applied.
Parent	The parent QSAP ID. If the parent ID is different than the QSAP ID, then the port is a member of a link aggregate or VFL.

Release History

Release 7.1.1; command was introduced.
Release 7.2.1; output display modified for the OmniSwitch 6900.
Release 7.2.1.R02; output display modified for the OmniSwitch 6900.
Release 8.3.1; **vf-link** and **summary** parameters added.

Related Commands

qos qsi qsp	Changes the QSet profile association for a QSet instance.
show qos qsi stats	Displays packet count statistics collected for a specific QSet instance.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsetInstanceTable
   alaVfcQsetId
   alaVfcQsetQsapId
   alaVfcQsetAdminState
   alaVfcQsetQSPId
   alaVfcQsetQSPName
   alaVfcQsetSchedulingMethod
   alaVfcQsetStatsAdmin
   alaVfcQsetStatsOper
alaVfcQInstanceTable
   alaVfcQInstanceQId
   alaVfcQInstanceCIRBandwidthLimitValue
   alaVfcQInstancePIRBandwidthLimitValue
   alaVfcQInstanceCIROperationalBandwidthLimitValue
   alaVfcQInstancePIROperationalBandwidthLimitValue
   alaVfcQInstanceStatsAdmin
   alaVfcQInstanceStatsOper
```

show qos qsi stats

Displays statistics for the QSet instance (QSI) queues that are associated with non-DCB (NDCB) ports.

show qos qsi {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} stats [bytes | rate [bytes]]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-15).
bytes	Displays the total number of bytes (instead of packets) that flow through the QSI queues. This parameter is not supported on the
rate	Displays the number of packets-per-second that flow through the QSI queues.

Defaults

parameter	default
bytes | rate	**bytes**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The specified port or link aggregate must have statistics collection enabled.
- Use the **port** *slot/port* or **linkagg** *agg_id* parameters to display QSI statistics associated with specific ports or link aggregates.
- It is possible to combine the **bytes** parameter with the **rate** parameter to display the number of bytes-per-second that flow through the QSI queues. For example, **show qos qsi port 1/20 stats rate bytes**.
- Statistics are displayed on a per-queue basis for each port. There are eight queues associated with a single QSet instance. Each queue is identified with a queue ID (1–8). Each port and link aggregate is associated with one QSet instance.

Examples

```
-> show qos qsi port 1/20 stats
              Total                Total
Port        Q  Tx                   Drop
------------+--+--------------------+--------------------
1/20        1  0                    0
1/20        2  0                    0
1/20        3  0                    0
1/20        4  0                    0
1/20        5  0                    0
1/20        6  0                    0
1/20        7  0                    0
1/20        8  9984                 0

-> show qos qsi port 1/20 stats bytes
              Total                Total
Port        Q  Tx                   Drop
------------+--+--------------------+--------------------
1/20        1  0                    0
1/20        2  0                    0
1/20        3  0                    0
1/20        4  0                    0
1/20        5  0                    0
1/20        6  0                    0
1/20        7  0                    0
1/20        8  987424               0

-> show qos qsi port 1/20 stats rate
              Average              Average
Port        Q  Tx/s                 Drop/s
------------+--+--------------------+--------------------
1/20        1  0                    0
1/20        2  0                    0
1/20        3  0                    0
1/20        4  0                    0
1/20        5  0                    0
1/20        6  0                    0
1/20        7  0                    0
1/20        8  7                    0

-> show qos qsi port 1/20 stats rate bytes
              Average              Average
Port        Q  Tx/s                 Drop/s
------------+--+--------------------+--------------------
1/20        1  0                    0
1/20        2  0                    0
1/20        3  0                    0
1/20        4  0                    0
1/20        5  0                    0
1/20        6  0                    0
1/20        7  0                    0
1/20        8  694                  0
```

output definitions

Port	The slot and port number.
Q	The QSet queue ID number (1–8) associated with the QoS (non-DCB) port.
Total Tx	Total packets or bytes transmitted.
Total Drop	Total packets or bytes dropped.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi stats	Enables or disables statistics collection for a DCB or non-DCB port.
clear qos qsi stats	Clears statistics collected for one or more QSet instances.

MIB Objects

```
alaVfcQInstanceTable
   alaVfcQInstancePacketsEnqueued
   alaVfcQInstanceBytesEnqueued
   alaVfcQInstancePacketsDropped
   alaVfcQInstanceBytesDropped
```

show qos qsi wred-stats

Displays the Weighted Random Early Detection (WRED) statistics for the QSet instance.

show qos qsi {port *chassis/slot/port***[**-*port2***] | slot** *slot* **| linkagg** *agg_id***[**-*agg_id2***]} wred-stats [rate | bytes]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number of a non-DCB (Data Center Bridging) port. Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number of a non-DCB aggregate. Use a hyphen to specify a range of IDs (10-15).
rate	Displays the number of packets per second.
bytes	Displays the total number of bytes.

Defaults

By default, displays the total number of packets for all the QSI queues.

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is not supported on OmniSwitch 6900 DCB ports.
- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to display QSI statistics associated with specific ports or link aggregates.
- This command displays the total number of packets or bytes.

Examples

```
-> show qos qsi port 1/2 wred-stats
* OS6900  WRED Per Q stats not supported, Tx stats not supported
             Green                Yellow                Red
Port        Q Drop                 Drop                  Drop
----------+-+--------------------+--------------------+--------------------
Port 1/2    - 0                   0                    0

-> show qos qsi port 1/1 wred-stats rate
* OS6900  WRED Per Q stats not supported, Tx stats not supported
              Green                Yellow               Red
Port        Q  Drop/s               Drop/s               Drop/s
----------+--+--------------------+--------------------+--------------------
1/1         -  0                   0                    0
```

```
-> show qos qsi port 1/1 wred-stats bytes
* OS6900  WRED Per Q stats not supported, Tx stats not supported
              Green               Yellow              Red
Port        Q  Drop                Drop                Drop
-----------+--+-------------------+-------------------+-------------------
1/1         -  0                   0                   0
```

output definitions

Port	The switch port.
Q	The egress queue ID (1–8) associated with the port.
Green TX, Green Drop	The number of green packets or bytes transmitted and dropped.
Yellow TX, Yellow Drop	The number of yellow packets or bytes transmitted and dropped.
Red TX, Red Drop	The number of red packets or bytes transmitted and dropped.

Release History

Release 7.2.1.R01; WRED per Q stats not supported; Tx stats not supported.

Related Commands

show qos qsi	Displays the QSet instance configuration.
clear qos qsi stats	Clears statistics collected for one or more QSet instances.

MIB Objects

```
alcatelIND1VfcMIB
 alaVfcQInstanceTable
   alaVfcQInstanceQId
   alaVfcQInstanceGreenPacketsAccepted
   alaVfcQInstanceGreenBytesAccepted
   alaVfcQInstanceGreenPacketsDropped
   alaVfcQInstanceGreenBytesDropped
   alaVfcQInstanceYellowPacketsAccepted
   alaVfcQInstanceYellowBytesAccepted
   alaVfcQInstanceYellowPacketsDropped
   alaVfcQInstanceYellowBytesDropped
   alaVfcQInstanceRedPacketsAccepted
   alaVfcQInstanceRedBytesAccepted
   alaVfcQInstanceRedPacketsDropped
   alaVfcQInstanceRedBytesDropped
```

show qos qsp system-default

Displays the name and ID of the QSet profile (QSP) that serves as the default system QSP. when the switch is running in the non-DCB (NDCB) mode.

show qos qsp system-default

Syntax Definitions

N/A

Defaults

By default, QSP 1 is assigned to each QSet instance.

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

- The switch is operating in the NDCB mode when the OmniSwitch Data Center software license is *not* installed on the switch.
- The switch is operating in the Data Center Bridging (DCB) mode when the OmniSwitch Data Center software license is installed on the switch. Configuring the system default profile is not supported in the DCB mode.

Examples

```
-> show qos qsp system-default
NDCB Default QSP profile          : 1   (qsp-1)
```

Release History

Release 8.3.1; command introduced.

Related Commands

qos qsp system-default	Configures the default QSet profile for the switch.

MIB Objects

```
alcatelIND1VfcMIB
   alaVfcSystemDefaultQsetQSPName
   alaVfcSystemDefaultQsetQSPId
```

clear qos qsi stats

Clears QSet instance (QSI) statistics.

clear qos qsi {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} stats**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (1\5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **port** *slot/port* and **linkagg** *agg_id* parameters to clear QSI statistics associated with specific ports or link aggregates.
- QSI statistics can only be cleared on ports or link aggregates that have statistics collection enabled.

Examples

```
-> clear qos qsi port 1/1/2 stats
-> clear qos qsi port 1/1/10-15 stats
-> clear qos qsi linkagg 5 stats
-> clear qos qsi linkagg 10-15 stats
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show qos qsi stats	Displays QSet instance statistics.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsapTable
   alaVfcQsapClearStats
   alaVfcQsapQpId
```

qos qsp dcb import

Imports a Data Center Bridging profile (DCP) to a new or previous custom profile.

qos qsp dcb {*dcp_id* **|** *dcp_name***} import qsp dcb {***import_dcp_id* **|** *import_dcp_name***} [802.3x-pause]**

no qos qsp dcb {*dcp_id* **|** *dcp_name***}**

Syntax Definitions

dcp_id	A DCB custom profile ID. The valid custom profile ID range is 12 through 128.
dcp_name	The DCB profile name.
import_dcp_id	The ID of the DCB profile to import. The valid profile ID range is 1–11 to specify a predefined profile and 12–128 to specify a custom profile.
import_dcp_name	The name of the DCB profile to import.
802.3x-pause	Makes the profile pause-ready. When enabled, the Priority based Flow Control (PFC) is lossy for all traffic classes in the profile and they cannot be changed to lossless.

Defaults

By default the **802.3x-pause** flag is disabled.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The new DCB profile must be unique and not contain the same name and ID of an existing DCB profile.
- On an OmniSwitch 6900-Q32, only import DCB profile 8 to create a custom profile. Do not use any of the other pre-defined profiles to create a custom profile.
- Use the **no** form of the command to remove an existing custom DCB profile from the switch configuration.
- The pre-defined DCB profiles from 1 to 11 cannot be removed from the switch configuration.
- A custom profile attached to a port cannot be removed from the switch configuration. In this case, the profile must be disassociated from the port before being removed.
- Use the **802.3x-pause** tag to enable pause-ready on the profile. When enabled, the PFC is lossy for all traffic classes in the profile and they cannot be changed to lossless. This type of custom profile is created to support legacy PAUSE frames on ports to which the profile is applied. However, before applying the custom profile to a port, disable PFC TLV and PFC willing on the port.

Examples

```
-> qos qsp dcb 33 import qsp dcb 8
-> qos qsp dcb lossyETS import qsp 10
```

```
-> qos qsp dcb 34 import qsp dcb 7 802.3x-pause
-> no qsp dcb 33
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsp dcb	Displays the configured DCB profile and the traffic classes associated to the DCB profile.
show qos qsi stats	Displays the queue statistics for DCB and Non-DCB (NDCB) ports.
clear qos qsi dcb pfc stats	Clears the port statistics.

MIB Objects

```
alaDcbxDCProfileTable
   alaDcbxDCPId
   alaDcbxDCPName
   alaDcbxDCPTemplateDCPId
   alaDcbxDCPTemplateDCPName
   alaDcbxDCP8023xPauseReady
   alaDcbxDCPRowStatus
```

qos qsp dcb tc

Modifies the Data Center Bridging (DCB) traffic class attributes of a DCB profile.

qos qsp dcb {*dcp_id* **|** *dcp_name***} tc** *tc_num* **{pfc flow-type { ll | nll} | pfc link-delay** *allowance* **| min-bw** *%* | **max-bw** *%* | **recommended bw** *%***}**

Syntax Definitions

dcp_id	A DCB custom profile ID. The valid custom profile ID range is 12 through 128.
dcp_name	The DCB custom profile name.
tc_num	The traffic class number in the DCB profile.
ll	Designates traffic class as lossless.
nll	Designates traffic class as non-lossless (lossy).
allowance	Link delay allowance value for PFC.
min-bw *%*	Sets the minimum bandwidth guaranteed for the Enhanced Transmission Selection (ETS) traffic class.
max-bw *%*	Sets the maximum bandwidth guaranteed for the Strict Priority (SP) traffic class.
recommended bw *%*	Sets the recommended minimum bandwidth for the traffic class.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The **pfc flow-type** option is used to change a traffic class from lossless (ll) to lossy (nll) or from lossy (nll) to lossless (ll).
- The **pfc link-delay** option sets the actual headroom for the traffic class. An incorrect setting can result in traffic loss.
- The **min-bw** option sets the minimum bandwidth guaranteed for the ETS traffic class.
- The **max-bw** option sets the maximum bandwidth guaranteed for the SP traffic class.
- The **recommended bw** option sets the recommended minimum bandwidth for the traffic class.

Examples

```
-> qos qsp dcb 11 tc 0 min-bw 3
-> qos qsp dcb lossyETS tc 1 min-bw 12
-> qos qsp dcb lossyETS tc 2 pfc flow-type ll
-> qos qsp dcb 11 tc 0 recommended bw 3
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsp dcb	Displays the configured DCB profiles and the traffic classes associated to the DCB profile.

MIB Objects

```
alaDcbxDCPTrafficClassTable
   alaDcbxDCPTCDCPId
   alaDcbxDCPTCTrafficClass
   alaDcbxDCPTCDCPName
   alaDcbxDCPTCPFCTrafficFlow
   alaDcbxDCPTCPFCLinkDelay
   alaDcbxDCPTCMinimumBandwidth
   alaDcbxDCPTCMaximumBandwidth
   alaDcbxDCPTCRecommendedBandwidth
```

qos qsp dcb tc-numbering

Modifies the traffic class (TC) numbering for custom profiles.

qos qsp dcb {*dcp_id* | *dcp_name***} tc-numbering** *tc_num*

Syntax Definitions

dcp_id	A DCB custom profile ID. The valid custom profile ID range is 12 through 128.
dcp_name	The DCB custom profile name.
tc_num	Enter the traffic class numbering sequence for the DCB profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The command can be used to modify the traffic class numbering for the custom profiles.
- The numbering must be assigned in ascending order. For example, a profile with TCs numbered 0, 1, 2, can be changed to 1, 5, 7.
- The number of TCs specified must match the number of TCs in the profile.

Examples

```
-> qos qsp dcb 11 tc-numbering 1 5 7 9
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsp dcb	Displays the configured DCB profiles and the traffic classes associated to the DCB profile.

MIB Objects

```
alaDcbxDCProfileTable
   alaDcbxDCPTCDCPName
   alaDcbxDCPTCsPresent
```

qos qsi qsp dcb

Assigns a DCB profile to a port or link aggregate.

qos qsi {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} qsp dcb {***dcp_id* **|** *dcb_name***}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
dcp_id	DCB profile ID. DCB profile ID 11 through 128 refers to the custom profiles. DCB profile ID 1 through 10 refers to the predefined profiles.
dcp_name	DCB profile name.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When a DCB profile is assigned to a link aggregate, the profile is applied to all the ports associated with the linkagg.
- Avoid configuring different profiles for each port of the link aggregate.
- The command will not work if the link aggregate is associated with 1Gig port. Different combination of ports (10G and 40G) are allowed in a link aggregate.

Examples

```
-> qos qsi port 1/11 qsp dcb lossyETS
-> qos qsi port 1/11 qsp dcb 7
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsp dcb	Displays the configured DCB profiles and the traffic classes associated with the DCB profile.

MIB Objects

```
alaDcbxPortInstanceEntry
   alaDcbxPIAdminDCPId
   alaDcbxPIAdminDCPName
```

qos qsi dcb dcbx version

Selects the version of the DCB Exchange protocol (DCBX) to apply to the specified DCB port.

qos qsi {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} dcb dcbx version {ieee | cee | auto}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
ieee	Selects IEEE 802.1Qaz DCBX.
cee	Selects Converged Enhanced Ethernet DCBX 1.01.
auto	Automatically detects the DCBX version used by the peer switch.

Defaults

By default, the DCB port is configured to automatically use the DCBX version detected from the peer.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Initially, the IEEE version of DCBX is run on the port until the switch detects the peer is running the CEE version. At that point, the switch will stop IEEE DCBX and start to run the CEE version.

Examples

```
-> qos qsi port 1/10 dcb dcbx version ieee
-> qos qsi port 1/10 dcb dcbx version cee
-> qos qsi port 1/11 dcb dcbx version auto
```

Release History

Release 7.3.3; command was introduced.

Related Commands

qos qsi dcb dcbx admin-state	Enables or disables DCBX functionality on the port.
qos qsi dcb dcbx ets	Enables or disables application Type, Length, Value (TLV) transmission on a per-port basis.
qos qsi dcb dcbx pfc	Enables or disables config-TLV, defense mode, and willing bit for PFC on a per-port basis.
show qos qsi dcb dcbx	Displays the DCBX configuration and status for the specified port.

MIB Objects

```
alaDcbxPortInstanceEntry
   alaDcbxPIDCBXVersion
```

qos qsi dcb dcbx admin-state

Enables or disables DCB exchange protocol (DCBX) functionality on a per port basis.

qos qsi {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} dcb dcbx admin-state {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
enable	Enables the DCBX functionality on the port.
disable	Disables the DCBX functionality on the port.

Defaults

parameter	default
dcbx admin-state	enable

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

The DCBX admin-state, enables or disables DBCX TLVs and negotiation on a port.

Examples

```
-> qos qsi port 1/10 dcb dcbx admin-state enable
-> qos qsi port 1/10 dcb dcbx admin-state disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi dcb dcbx version	Selects the version of DCBX to apply to the specified DCB port.
qos qsi dcb dcbx ets	Enables or disables application Type, Length, Value (TLV) transmission on a per port basis.
qos qsi dcb dcbx pfc	Enables or disables config-TLV, defense mode, and willing bit for PFC on a per port basis.
show qos qsi dcb dcbx	Displays the configured ports in the system and the related DCBX information.

MIB Objects

```
alaDcbxPortInstanceEntry
   alaDcbxPIIfIndex
   alaDcbxPIDCBXAdmin
```

qos qsi dcb dcbx ets

Enables or disables config-TLV, recommended-TLV, and the willing bit for ETS on a per-port basis.

qos qsi {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} dcb dcbx ets [config-tlv {enable | disable} | recommend-tlv {enable | disable} | willing {yes | no}]**

Syntax Definitions

chassis	The chassis identifier.
slot/port[-port2]	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
config-tlv enable	Enables the transmission of ETS configuration TLVs.
config-tlv disable	Disables the transmission of ETS configuration TLVs.
recommend-tlv enable	Enables the transmission of ETS recommended TLVs.
recommend-tlv disable	Disables the transmission of ETS recommended TLVs.
yes	Sets the willing bit to on in the TLVs.
no	Sets the willing bit to off in the TLVs.

Defaults

parameter	default
config-tlv {enable | disable}	enable
ets recommend-tlv {enable | disable}	enable
willing {yes | no}	yes

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the option **ets config-tlv** to enable or disable the transmission of ETS configuration TLVs. To use this option, DCBX must be enabled on the port.
- Use the option **ets recommended-tlv** to enable or disable the transmission of ETS recommended TLVs. To use this option, DCBX must be enabled on the port.
- Use the option **ets willing** to set the willing bit on the TLVs. This option is used when the DCBX is enabled on the port and the ETS configuration TLV is sent on the port.

Examples

```
-> qos qsi port 1/1-10 dcb dcbx ets config-tlv disable
-> qos qsi port 1/11 dcb dcbx ets recommended-tlv disable
-> qos qsi linkagg 5 dcb dcbx ets willing no
```

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi dcb dcbx version	Selects the version of DCBX to apply to the specified DCB port.
qos qsi dcb dcbx admin-state	Enables or disables DCBX functionality for the port.
qos qsi dcb dcbx pfc	Enables or disables config-TLV, defense mode, and willing bit for PFC on a per port basis.
show qos qsi dcb dcbx	Displays the configured ports in the system and the related DCBX information.
show qos qsi dcb ets	Displays the configured ports in the system and the related DCBX ETS and ETS traffic class information.

MIB Objects

```
lldpXdot1dcbxConfigETSConfigurationTable
lldpXdot1dcbxConfigETSRecommendationTable
lldpXdot1dcbxLocETSBasicConfigurationTable
   lldpXdot1dcbxConfigETSConfigurationTxEnable
   lldpXdot1dcbxConfigETSRecommendationTxEnable
   lldpXdot1dcbxLocETSConWilling
```

qos qsi dcb dcbx pfc

Enables or disables config-TLV, defense mode, and willing for PFC on a per port basis.

qos qsi {port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} dcb dcbx pfc [config-tlv {enable | disable} | defense {enable | disable} | willing {yes | no}]**

Syntax Definitions

chassis	The chassis identifier.
slot/port[-port2]	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[-***agg_id2***]**	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
config-tlv enable	Enables the transmission of PFC configuration TLVs.
config-tlv disable	Disables the transmission of PFC configuration TLVs.
defense enable	Enables the defense mode for the PFC.
defense disable	Disables the defense mode for the PFC.
willing yes	Allows the PFC to negotiate with the network.
willing no	Stops the PFC from negotiating with the network.

Defaults

parameter	default
pfc config-tlv	enable
pfc defense	enable
pfc willing	yes

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the option **pfc config-tlv** to enable or disable the transmission of PFC configuration TLVs. To use this option, DCBX must be enabled on the port.
- Use the option **ets willing** to allow the PFC to negotiate with the network.

Examples

```
-> qos qsi port 1/1-10 dcb dcbx pfc config-tlv disable
-> qos qsi port 1/11 dcb dcbx pfc defense disable
-> qos qsi linkagg 5 dcb dcbx pfc willing no
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsi dcbx pfc	Displays the configured ports in the system and the related DCBX PFC information.
show qos pfc-lossless-usage	Displays the usage of the PFC lossless traffic class on the switch.
show qos qsi dcb pfc stats	Displays the traffic statistics per port and per traffic class.

MIB Objects

```
lldpXdot1dcbxConfigPFCTable
   lldpXdot1dcbxConfigPFCTxEnable
   alaDcbxPIPFCDefense
   lldpXdot1dcbxLocPFCWilling
```

show qos qsp dcb

Displays the configured DCB profiles and the traffic classes associated with the DCB profile.

show qos qsp dcb [*dcp_id* **|** *dcp_name***] [tc** *tc_num***]**

Syntax Definitions

dcp_id	DCB profile ID. DCB profile ID 11–128 refers to the custom profiles. DCB profile ID 1–0 refers to the predefined profiles.
dcp_name	DCB profile name.
tc_num	The traffic class associated to the DCB profile. The valid range is 0–7.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- This command displays the details of the configured DCB profile.
- Use the **tc** option to display the traffic classes associated to the DCB profile.

Examples

```
-> show qos qsp dcb

Legends: Prio TC Map:
            Represents the priority to traffic class mapping;
            begins with priority 0 on the left and displays the
            traffic class it belongs to.

                                ETS
                 Priority PFC Max Template-DCP       802.3x
#   Name         TC Map   Cap TC  #   Name         Pause-Ready
---+------------+--------+---+---+---+------------+-----------
1   dcp-1        00001122 8   8   1   dcp-1        No
2   dcp-2        00112233 8   8   2   dcp-2        No
3   dcp-3        00112234 8   8   3   dcp-3        No
4   dcp-4        10223345 8   8   4   dcp-4        No
5   dcp-5        10234456 8   8   5   dcp-5        No
6   dcp-6        10234567 8   8   6   dcp-6        No
7   dcp-7        01234567 8   8   7   dcp-7        No
8   dcp-8        01234567 8   8   8   dcp-8        No
9   dcp-9        10234567 8   8   9   dcp-9        No
10  dcp-10       10234567 8   8   10  dcp-10       No
20  dcp-20       10234567 8   8   10  dcp-10       No
```

output definitions

#	Indicates a DCB profile entry.
Name	Name of the DCB profile.
Priority TC Map	Indicates the priority of the traffic class.
PFC Cap	Indicates the number of traffic classes on the local device that have simultaneously PFC enabled.
ETS Max TC	Indicates the number of traffic classes supported.
Template-DCP #	Identifies the template DCB profile.
Template-DCP Name	Name of the template DCB profile.
802.3x Pause-Ready	Indicates if pause-ready is enabled for the profile.

```
-> show qos qsp dcp tc

Legends: Linkdelay shown in KB.
         * denotes user modified value

                                ETS ETS       ETS  ETS
                                Min Max ETS   Reco Reco  PFC  PFC
#   Name         TC Priorities BW  BW  Sched BW   Sched Mode LinkDelay
---+------------+--+----------+---+---+-----+----+-----+----+---------
1   Dft_1        0  4567       0   100 SP    0    SP    nLL  0
1   Dft_1        1  23         50  100 ETS   50   ETS   LL   80*
1   Dft_1        2  01         50  100 ETS   50   ETS   LL   60
```

output definitions

#	Indicates a DCB profile entry.
Name	Name of DCB profile.
TC	Indicates the traffic class.
Priorities	Indicates the priorities assigned to the traffic class.
ETS Min BW	Indicates the minimum bandwidth assigned to the traffic class.
ETS Max BW	Indicates the maximum bandwidth assigned to the traffic class.
ETS Sched	Indicates the traffic class scheduler assigned to the traffic class.
ETS Reco BW	Indicates the recommended minimum bandwidth assigned to the traffic class.
ETS Reco Sched	Indicates the recommended traffic class scheduler assigned to the traffic class.
PFC Mode	Indicates if PFC traffic flow is enabled on the traffic class.
PFC LinkDelay	Indicates the delay in the PFC link.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsp dcb import	Imports a data center profile to a new or old custom DCB profile.
clear qos qsi stats	Modifies the Data Center Bridging Capabilities Exchange Protocols (DCBX) control portion of a DCB profile.
qos qsp dcb tc	Modifies the Data Center Bridging (DCB) attributes of a DCB profile.
qos qsp dcb tc-numbering	Modifies the priority of traffic class mapping the custom profiles.
clear qos qsi dcb pfc stats	Clears the port statistics.

MIB Objects

```
alaDcbxDCProfileTable
   alaDcbxDCPId
   alaDcbxDCPName
   alaDcbxDCPPriorityTCMap
   alaDcbxDCPPFCCap
   alaDcbxDCPETSTrafficClassesSupported
   alaDcbxDCPTemplateDCPId
   alaDcbxDCPTemplateDCPName
   alaDcbxDCP8023xPauseReady
 alaDcbxDCPTrafficClassTable
   alaDcbxDCPTCDCPId
   alaDcbxDCPTCDCPName
   alaDcbxDCPTCTrafficClass
   alaDcbxDCPTCPriorityMap
   alaDcbxDCPTCMinimumBandwidth
   alaDcbxDCPTCMaximumBandwidth
   alaDcbxDCPTCTrafficScheduler
   alaDcbxDCPTCRecommendedBandwidth
   alaDcbxDCPTCRecommendedTrafficScheduler
   alaDcbxDCPTCPFCTrafficFlow
   alaDcbxDCPTCPFCLinkDelay
```

show qos qsi dcb dcbx

Displays the DCBX port configuration and status.

show qos qsi [port *chassis/slot/port***[**-*port2*****] | linkagg** *agg_id***[**-*agg_id2*****]] dcb dcbx [status]**

Syntax Definitions

chassis	The chassis identifier.
slot/port[-*port2*]	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
status	Displays the DCBX operational status for the port.

Defaults

By default, the DCBX configuration is displayed for all ports.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **port** *slot/port* or **linkagg** *agg_id*, parameters to display information for a specific port or link aggregate.
- Use the **status** option to display the status information of the DCBX related to the port.

Examples

```
-> show qos qsi port 1/1-5 dcb dcbx
                                                                ETS
                         DCBX DCBX  Stats PFC     PFC PFC  Cfg Reco ETS
Port    DCP Name         Ver  Admin Admin Defense TLV Will TLV TLV  Will
------+---+------------+----+-----+-----+-------+---+----+---+----+----
1/1     8   dcp-8        AUTO Ena   Dis   Ena     Ena Yes  Ena Ena  Yes
1/2     8   dcp-8        AUTO Ena   Dis   Ena     Ena Yes  Ena Ena  Yes
1/3     8   dcp-8        AUTO Ena   Dis   Ena     Ena Yes  Ena Ena  Yes
1/4     8   dcp-8        AUTO Ena   Dis   Ena     Ena Yes  Ena Ena  Yes
1/5     8   dcp-8        AUTO Ena   Dis   Ena     Ena Yes  Ena Ena  Yes
```

output definitions

Port	The DCB slot and port number or link aggregate ID.
DCP	The DCB profile ID assigned to the port.
Name	The name of the DCB profile assigned to the port.
DCBX Ver	The version of DCBX running on the port (**CEE**, **IEEE**, or **AUTO**).
DCBX Admin	Indicates the administrative status of DCBX on the port.
Stats Admin	Indicates if statistics collection is enabled or disabled on the port.

output definitions (continued)

PFC Defense	Indicates the status of PFC defense (**Ena** or **Dis**). Applies when PFC negotiation fails. If enabled then PFC becomes disabled but traffic still flows. If disabled then the PFC local configuration remains on the port.
PFC TLV	Indicates whether the IEEE 802.1 organizationally defined PFC TLV transmission is allowed on a given LLDP transmission capable port.
PFC Will	Indicates whether or not the port is willing to accept the PFC configuration from a remote peer.
Cfg TLV	Indicates whether or not ETS configuration TLV transmission is allowed on a port.
Reco TLV	Indicates whether or not ETS configuration TLV transmission is allowed on a port.
ETS Will	Indicates whether or not the port is willing to accept the recommended ETS configuration from a remote peer.

```
-> show qos qsi port 1/1-5 dcb dcbx status
                         DCBX
              Local   Local Remote
         DCBX Oper    Oper  Oper
Port     Oper Changed Ver   Ver    Error                      Action
-------+----+-------+-----+------+--------------------------+----------------------
1/1      Dis  No      AUTO  -      No                         -
1/2      Dis  No      AUTO  -      No                         -
1/3      Dis  No      AUTO  -      No                         -
1/4      Dis  No      AUTO  -      No                         -
1/5      Dis  No      AUTO  -      No                         -
```

output definitions

Port	The DCB slot and port number or link aggregate ID.
DCBX Oper	Indicates the operational status of DCBX on the port.
Local Oper Changed	Identifies if the local configuration is different from the configuration imported from the DCB profile applied to the port.
Error	Indicates if there is an error condition.
Local Oper Ver	The version of DCBX running on the local port (**CEE**, **IEEE**, or **AUTO**).
Remote Oper Ver	The version of DCBX running on the remote port (**CEE**, **IEEE**, or **AUTO**).
Action	Indicates the action taken as a result of the status.

Release History

Release 7.3.1; command was introduced.
Release 7.3.3; fields added to display the version of DCBX (IEEE or CEE).

Related Commands

qos qsi qsp dcb	Assigns a DCB profile to a port or link aggregate.
qos qsi dcb dcbx version	Configures the version of DCBX to run on the port (IEEE or CEE).
qos qsi dcb dcbx admin-state	Enables or disables DCBX functionality on a per port basis.
qos qsi stats	Enables or disables statistics collection.

MIB Objects

```
alaDcbxPortInstanceEntry
   alaDcbxPIIfIndex
   alaDcbxPIDCBXAdmin
   alaDcbxPIDCBXOper
   alaDcbxPIAdminDCPId
   alaDcbxPIAdminDCPName
   alaDcbxPILocalModified
   alaDcbxPIPFCDefense
   alaDcbxPIPFCStatsClear
   alaDcbxPIStatus
   alaDcbxPIActionTaken
   alaDcbxPIRowStatus
   alaDcbxPIDCBXVersion
   alaDcbxPIDCBXVersionOper
alaDcbxPortInstanceGroup
   alaDcbxPIDCBXAdmin,
   alaDcbxPIDCBXOper,
   alaDcbxPIAdminDCPId,
   alaDcbxPIAdminDCPName,
   alaDcbxPILocalModified,
   alaDcbxPIPFCDefense,
   alaDcbxPIPFCStatsClear,
   alaDcbxPIStatus,
   alaDcbxPIActionTaken,
   alaDcbxPIRowStatus,
   alaDcbxPIDCBXVersion,
   alaDcbxPIDCBXVersionOper
```

show qos qsi dcb ets

Displays the configured ports in the system and the related DCBX ETS and ETS traffic class information.

show qos qsi {port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} dcb ets [tc [***tc_num***]]**

Syntax Definitions

chassis	The chassis identifier.
slot/port[-*port2*]	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[-***agg_id2***]**	A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
tc_num	Enter the traffic class for which the information needs to be displayed. The valid range is 0–7.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the *tc_num* option to display the DCBX ETS information for a specific traffic class.

Examples

```
-> show qos qsi port 1/1 dcb ets
Legends: Prio TC Map:
            Represents the priority to traffic class mapping;
            begins with priority 0 on the left and displays the
            traffic class it belongs to.
          * indicates port oper status is different than the configured status

           Loc-Adm    Loc-Adm     Loc-Oper    Loc-Oper    Rem-Oper    Rem-Oper
       Prio      Max           Prio      Max           Prio      Max
Port   TC Map    TC  CBS  Will TC Map    TC  CBS  Will TC Map    TC  CBS  Will
------+---------+---+----+----+---------+---+----+----+---------+---+----+----
  1/1  00111222  3   Dis  Yes  00111222  3   Dis  Yes  00111222  3   Ena  Ena
```

output definitions

Port	Configured DCB ports.
Loc-Adm Prio TC Map	Indicates the traffic class to which the priority is to be assigned.
Loc-Adm Max TC	Indicates the number of traffic classes supported.
Loc-Adm CBS	Indicates the status of the credit-based shaper traffic support.
Loc-Adm Will	Indicates if the local system is willing to accept the ETS configuration recommended by the remote system.
Loc-Oper Prio TC Map	Indicates the traffic class the priority belongs to.

output definitions (continued)

Loc-Oper Max TC	Indicates the number of traffic classes supported in the local system.
Loc-Oper CBS	Indicates if the credit-based shaper traffic is supported on the local system.
Loc-Oper Will	Indicates if the credit-based shaper traffic selection is supported on the local system.
Rem-Oper Prio TC Map	Indicates the priority that is assigned to a traffic class.
Rem-Oper Max TC	Indicates the number of traffic classes supported in the remote system.
Rem-Oper CBS	Indicates if the credit-based shaper traffic selection is supported on the remote system.
Rem-Oper Will	Indicates if the remote system is willing to accept the ETS configuration recommended by the remote system.

```
-> show qos qsi port 1/1 dcb ets tc

Legends: * indicates port oper status is different than the configured status

           Loc-Adm    Loc-Adm    Loc-Adm   Loc-Oper   Loc-Oper   Loc-Oper   Rem-Oper   Rem-Reco
                                 Reco Reco                        Reco Reco
Port    TC Priorities BW  Sched BW   Sched Priorities BW   Sched BW   Sched Priorities BW  Sched
-------+--+----------+---+-----+----+-----+----------+----+-----+----+-----+----------+---+-----
  1/1   0  01         0   SP    0    SP    01         0    SP    0    SP    01         0   SP
  1/1   1  23         50  ETS   50   ETS   23         50   ETS   50   ETS   23         50  ETS
  1/1   2  4567       50  ETS   50   ETS   4567       50   ETS   50   ETS   4567       50  ETS
```

output definitions

Port	Configured DCB ports.
TC	Indicates the traffic class the priority belongs to.
Loc-Adm Priorities	Indicates the priority assigned to the traffic class in the local system.
Loc-Adm BW	Indicates the bandwidth assignment to the traffic class in the local system.
Loc-Adm Sched	Indicates the traffic selection assignment to the traffic class in the local system.
Loc-Adm Reco BW	Indicates the traffic class to bandwidth assignment in the local system.
Loc-Adm Reco Sched	Indicates the traffic class to traffic selection assignment in the local system.
Loc-Oper Priorities	Indicates the priority assigned to the traffic class in the local system.
Loc-Oper BW	Indicates the bandwidth assigned to the traffic class in the local system.
Loc-Oper Sched	Indicates the traffic class to traffic selection assignment in the local system.
Loc-Oper Reco BW	Indicates the traffic class to bandwidth assignment in the local system.
Loc-Oper Reco Sched	Indicates the priority to traffic selection assignment in the local system.
Rem-Oper Priorities	Indicates the priority assigned to the traffic class in the remote system.
Rem-Oper BW	Indicates the traffic class to bandwidth assignment in the remote system.
Rem-Oper Sched	Indicates the traffic class to traffic selection assignment in the remote system.

output definitions (continued)

Rem-Oper Reco BW	Indicates the traffic class to bandwidth assignment in the remote system.
Rem-Oper Reco Sched	Indicates the priority to traffic selection assignment in the remote system.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi dcb dcbx ets	Enables or disables config-tlv, recommended-tlv, and willing for ETS on a per port basis.

MIB Objects

```
lldpXdot1dcbxAdminETSConPriorityAssignmentTable
lldpXdot1dcbxAdminETSBasicConfigurationTable
lldpXdot1dcbxLocETSConPriorityAssignmentTable
lldpXdot1dcbxLocETSBasicConfigurationTable
lldpXdot1dcbxRemETSConPriorityAssignmentTable
lldpXdot1dcbxRemETSBasicConfigurationTable
   lldpV2LocPortIfIndex
   lldpXdot1dcbxAdminETSConPriTrafficClass
   lldpXdot1dcbxAdminETSConTrafficClassesSupported
   lldpXdot1dcbxAdminETSConCreditBasedShaperSupport
   lldpXdot1dcbxAdminETSConWilling
   lldpXdot1dcbxLocETSConPriTrafficClass
   lldpXdot1dcbxLocETSConTrafficClassesSupported
   lldpXdot1dcbxLocETSConCreditBasedShaperSupport
   lldpXdot1dcbxLocETSConWilling
   lldpXdot1dcbxRemETSConPriTrafficClass
   lldpXdot1dcbxRemETSConTrafficClassesSupported
   lldpXdot1dcbxRemETSConCreditBasedShaperSupport
   lldpXdot1dcbxRemETSConWilling
lldpXdot1dcbxAdminETSConTrafficClassBandwidthTable
lldpXdot1dcbxAdminETSConTrafficSelectionAlgorithmTable
lldpXdot1dcbxAdminETSRecoTrafficClassBandwidthTable
lldpXdot1dcbxAdminETSRecoTrafficSelectionAlgorithmTable
lldpXdot1dcbxLocETSConTrafficClassBandwidthTable
lldpXdot1dcbxLocETSConTrafficSelectionAlgorithmTable
lldpXdot1dcbxLocETSRecoTrafficClassBandwidthTable
lldpXdot1dcbxLocETSRecoTrafficSelectionAlgorithmTable
lldpXdot1dcbxRemETSConTrafficClassBandwidthTable
lldpXdot1dcbxRemETSConTrafficSelectionAlgorithmTable
lldpXdot1dcbxRemETSRecoTrafficClassBandwidthTable
lldpXdot1dcbxRemETSRecoTrafficSelectionAlgorithmTable
   lldpV2LocPortIfIndex
   lldpXdot1dcbxAdminETSConTrafficClass
```

```
lldpXdot1dcbxAdminETSConTrafficClassBandwidth
lldpXdot1dcbxAdminETSConTrafficSelectionAlgorithm
lldpXdot1dcbxAdminETSRecoTrafficClassBandwidth
lldpXdot1dcbxAdminETSRecoTrafficSelectionAlgorithm
lldpXdot1dcbxLocETSConTrafficClassBandwidth
lldpXdot1dcbxLocETSConTrafficSelectionAlgorithm
lldpXdot1dcbxLocETSRecoTrafficClassBandwidth
lldpXdot1dcbxLocETSRecoTrafficSelectionAlgorithm
lldpXdot1dcbxRemETSConTrafficClassBandwidth
lldpXdot1dcbxRemETSConTrafficSelectionAlgorithm
lldpXdot1dcbxRemETSRecoTrafficClassBandwidth
lldpXdot1dcbxRemETSRecoTrafficSelectionAlgorithm
```

show qos qsi dcbx pfc

Displays the configured ports in the system and the related DCBX PFC information.

show qos qsi {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} dcb pfc**

Syntax Definitions

chassis	The chassis identifier.
slot/port[-*port2*]	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

If there is no PFC TLV received from the remote end, then the remote information will be blank.

Examples

```
-> show qos qsi port 4/1-2 dcb pfc

Legends: * indicates port oper status is different than the configured status

               Loc-Adm  Loc-Adm       Loc-Oper Loc-Oper       Rem-Oper Rem-Oper
Port    Priorities MBC Will Cap Priorities MBC Will Cap Priorities MBC Will Cap
-------+----------+---+----+---+----------+---+----+---+----------+---+----+---
  4/1*  0467       No  Yes  3   01         No  No   3   01         Yes No   3
  4/2*  23         No  No   3   -          No  No   3   -          Yes No   3
```

output definitions

Port	Configured DCB ports.
Loc-Adm Priorities	Indicates the priority for which PFC is enabled or disabled.
Loc-Adm MBC	Indicates if the local system is capable of bypassing MACsec processing when MACsec is disabled.
Loc-Adm Will	Indicates if the local system is willing to accept the PFC configuration of the remote system.
Loc-Adm Cap	Indicates the number of traffic classes on the local device that have simultaneously PFC enabled.
Loc-Oper Priorities	Indicates if PFC is enabled on the corresponding priority.
Loc-Oper MBC	Indicates if the local system is capable of bypassing MACsec processing when MACsec is disabled.

output definitions (continued)

Loc-Oper Will	Indicates if the local system is willing to accept the PFC configuration of the remote system.
Loc-Oper Cap	Indicates the number of traffic classes on the local device that have simultaneously PFC enabled.
Rem-Oper Priorities	Indicates if PFC is enabled on the corresponding priority on the remote system.
Rem-Oper MBC	Indicates if the remote system is capable of bypassing MACsec processing when MACsec is disabled.
Rem-Oper Will	Indicates if the remote system is willing to accept the PFC configuration of the local system.
Rem-Oper Cap	Indicates the number of traffic classes on the remote device that have simultaneously PFC enabled.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi dcb dcbx pfc	Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis.

MIB Objects

```
lldpXdot1dcbxAdminPFCEnableTable
lldpXdot1dcbxAdminPFCBasicTable
lldpXdot1dcbxLocPFCEnableTable
lldpXdot1dcbxLocPFCBasicTable
lldpXdot1dcbxRemPFCEnableTable
lldpXdot1dcbxRemPFCBasicTable
   lldpV2LocPortIfIndex
   lldpXdot1dcbxAdminPFCEnableEnabled
   lldpXdot1dcbxAdminPFCMBC
   lldpXdot1dcbxAdminPFCWilling
   lldpXdot1dcbxAdminPFCCap
   lldpXdot1dcbxLocPFCEnableEnabled
   lldpXdot1dcbxLocPFCMBC
   lldpXdot1dcbxLocPFCWilling
   lldpXdot1dcbxLocPFCCap
   lldpXdot1dcbxRemPFCEnableEnabled
   lldpXdot1dcbxRemPFCMBC
   lldpXdot1dcbxRemPFCWilling
   lldpXdot1dcbxRemPFCCap
```

show qos pfc-lossless-usage

Displays the usage of the PFC lossless traffic class on the switch.

show qos pfc-lossless-usage

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

This command displays the PFC lossless traffic class usage on the switch.

Examples

```
-> show qos pfc-lossless-usage
Lossless Priorities in use     : 55,
Lossless Priorities reserved   : 60,
Lossless Priorities available  : 73
```

output definitions

Lossless Priorities in use	Indicates the number of PFC lossless priorities in use in the system.
Lossless Priorities reserved	Indicates the number of PFC lossless priorities in reserve in the system.
Lossless Priorities available	Indicates the number of priorities available to be configured as PFC lossless.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi dcb dcbx pfc	Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis.

MIB Objects

```
alaDcbxConfig
   alaDcbxPfcLLPrioritiesUsed
   alaDcbxPfcLLPrioritiesReserved
   alaDcbxPfcLLPrioritiesAvailable
```

show qos qsi dcb pfc stats

Displays the Priority Flow Control (PFC) statistics for the specified DCB port.

show qos qsi [port *chassis/slot/port***[-***port2***] dcb pfc stats**

Syntax Definitions

chassis	The chassis identifier.
slot/port[-*port2*]	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Statistics are displayed on a per-traffic class (TC) basis.

Examples

```
-> show qos qsi port 1/11 dcb pfc stats

Legends: displays packet count

              PFC                  PFC
Port    Q  TC TX (req)             RX (ind)
-------+--+--+--------------------+-------------------
1/11    0  0  0                    0
1/11    1  0  0                    0
1/11    2  0  0                    0
1/11    3  0  0                    0
1/11    4  1  0                    0
1/11    5  1  0                    0
1/11    6  2  0                    0
1/11    7  2  0                    0
```

output definitions

Port	The DCB port number.
Q	The 802.1p priority number (0–7). This number is mapped to a traffic class (TC) based on the DCB profile assigned to the port.
TC	Indicates the traffic class to which the priority belongs.
Priority	Indicates the priority of the DCB port.
PFC TX (req)	Total count of PFC packets transmitted.
PFC RX (ind)	Total count of PFC packets received.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi dcb dcbx pfc	Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis.
clear qos qsi dcb pfc stats	Clears the port statistics.

MIB Objects

```
alaDcbxPIPriorityTable
   alaDcbxPIPrioIfIndex
   alaDcbxPIPrioTC
   alaDcbxPIPrioPriority
   alaDcbxPIPrioPFCPacketsTransmitted
   alaDcbxPIPrioPFCPacketsReceived
```

clear qos qsi dcb pfc stats

Clears the DCB PFC queue statistics.

clear qos qsi {port *chassis/slot/port***[**-*port2***]} dcb pfc stats**

Syntax Definitions

chassis	The chassis identifier.
slot/port[-*port2*]	The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the *slot/port* parameter to clear queue statistics associated with specific ports.

Examples

```
-> clear qos qsi port 2/1 dcb pfc stats
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsi stats	Displays the queue statistics for DCB and NDCB ports.

MIB Objects

```
alaVfcQsetInstanceTable
   alaVfcQsetStatsClear
```

36 QoS Policy Commands

This chapter describes the CLI commands used for policy management in the switch. The Quality of Service (QoS) software in the switch uses policy rules for classifying incoming flows and deciding how to treat outgoing flows. A policy rule is made up of a policy condition and a policy action. Policy rules may be created on the switch through CLI or SNMP commands, or they may be created through the PolicyView GUI application on an attached LDAP server.

Note. Rules created through PolicyView cannot be modified through the CLI; however, you can create policies in the CLI that take precedence over policies created through PolicyView.

Refer to Chapter 35, "QoS Commands," for information about commands used to configure QoS software.

MIB information for the QoS policy commands is as follows:

Filename: ALCATEL-IND1-QOS-MIB.mib
Module alaQoSMIB

Important Note. Some of the commands listed here are not currently supported on one or more platforms. See command descriptions in this chapter and check release notes for information about commands that are not supported.

The QoS Policy commands are listed here:

Policy commands	**policy rule** **policy validity-period** **policy list** **policy list rules** **policy condition** **policy action** **show policy action** **show policy condition** **show active policy rule** **show policy rule** **show policy validity period** **show active policy list** **show policy list** **show policy ipv4-summary** **show policy ipv6-summary**

Group commands	**policy network group** **policy service** **policy service group** **policy mac group** **policy port group** **policy map group** **show policy network group** **show policy mac group** **show policy port group** **show policy map group** **show policy service** **show policy service group**
Condition commands	**policy condition** **policy condition source ip** **policy condition source ipv6** **policy condition destination ip** **policy condition destination ipv6** **policy condition multicast ip** **policy condition source network group** **policy condition destination network group** **policy condition multicast network group** **policy condition source ip-port** **policy condition destination ip-port** **policy condition source tcp-port** **policy condition destination tcp-port** **policy condition source udp-port** **policy condition destination udp-port** **policy condition ethertype** **policy condition established** **policy condition tcpflags** **policy condition service** **policy condition service group** **policy condition icmptype** **policy condition icmpcode** **policy condition ip-protocol** **policy condition ipv6** **policy condition flow-label** **policy condition tos** **policy condition dscp** **policy condition source mac** **policy condition destination mac** **policy condition source mac group** **policy condition destination mac group** **policy condition source vlan** **policy condition inner source-vlan** **policy condition destination vlan** **policy condition 802.1p** **policy condition inner 802.1p** **policy condition source port** **policy condition destination port** **policy condition source port group** **policy condition destination port group** **policy condition vrf** **policy condition fragments** **policy condition appfp-group**

Action commands	**policy action** **policy action disposition** **policy action shared** **policy action priority** **policy action maximum bandwidth** **policy action maximum depth** **policy action cir** **policy action cpu priority** **policy action tos** **policy action 802.1p** **policy action dscp** **policy action map** **policy action permanent gateway-ip** **policy action permanent gateway-ipv6** **policy action port-disable** **policy action redirect port** **policy action redirect linkagg** **policy action no-cache** **policy action mirror**

Types of policies are generally determined by the kind of traffic they classify (policy conditions) and how the policy is enforced (policy actions). Commands used for particular types of policies are listed here. See the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about creating these types of policies and information about valid condition/action combinations.

Access Control Lists	**policy condition** **policy action disposition** **policy rule**
Traffic prioritization/shaping	**policy action shared** **policy action priority** **policy action maximum bandwidth** **policy rule**
802.1p/ToS/DSCP tagging or mapping	**policy condition tos** **policy condition dscp** **policy condition 802.1p** **policy action tos** **policy action 802.1p** **policy action dscp** **policy action map** **policy rule**
Policy based port mirroring	**policy action mirror**
VLAN Stacking	**policy condition inner source-vlan** **policy condition inner 802.1p**
VXLAN Snooping	**policy condition vxlan** **policy condition vxlan inner source mac** **policy condition vxlan inner source mac-group** **policy condition vxlan inner source ip** **policy condition vxlan inner source ipv6** **policy condition vxlan inner ip-protocol** **policy condition vxlan inner l4-port** **policy condition vxlan vxlan-port**

policy rule

Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

policy rule *rule_name* **[enable | disable] [precedence** *precedence***] [condition** *condition***] [action** *action***] [validity-period** *name***] [save] [log [log-interval** *seconds***]] [count {packets | bytes}] [trap] [default-list]**

policy rule *rule_name* **no {validity-period | save | log | trap | default-list}**

no policy rule *rule_name*

Syntax Definitions

rule_name	The name of the policy rule, any alphanumeric string.
enable	Enables the policy rule.
disable	Disables the policy rule.
precedence	The precedence value in the range 0–65535. This value determines the order in which rules are searched for a matching condition. A higher number indicates higher precedence. Typically the range 30000–65535 is reserved for PolicyView.
condition	The condition name that is associated with this rule. Conditions are configured through the **policy condition** command.
action	The name of the action that is associated with this rule. Actions are configured through the **policy action** command.
name	The name of a user-defined validity period that is associated with this rule. Validity periods are configured through the **policy validity period** command.
save	Marks the policy rule so that it may be captured as part of the switch configuration.
log	Configures the switch to log messages about specific flows coming into the switch that match this policy rule. *This parameter is not supported on the OmniSwitch 6465 or OmniSwitch 6560.*
seconds	Configures how often to look for packets that match this policy rule when rule logging is applied (in the range from 0–3600 seconds). A value of 0 specifies to log as often as possible.
packets	Counts the number of packets that match the rule.
bytes	Counts the number of bytes that match the rule.
trap	Enables or disables traps for the rule.
default-list	Adds the rule to the QoS default policy list.

Defaults

parameter	default
enable | disable	enable
precedence	0
log	no
seconds	60
packets | bytes	packets
trap	enable
default-list	adds rule to the default list

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Any rule configured through this command is not active on the switch until the **qos apply** command is issued.
- A policy rule configured through the PolicyView application may not be edited in the CLI. You may, however, create a rule using the CLI with a higher precedence that will override a rule created through PolicyView.
- Use the **no** form of the command to remove the rule from the configuration or to remove parameters from a particular rule. The change will not take effect, however, until the **qos apply** command is issued.
- Only one validity period is associated with a policy rule. Each time this command is entered with a validity period name specified, the existing period name is overwritten with the new one.
- Software and hardware resources are allocated for rules associated with a validity period even if the validity period is not active. Pre-allocating the resources makes sure the rule can be enforced when the validity period becomes active.
- The **save** option marks the policy rule so that the rule will be captured in an ASCII text file (using the **configuration snapshot** command), saved to the working directory after the **write memory** command or **copy running-config working** command is entered, or saved after a reboot. Rules are saved by default. If **no save** is entered for the rule, the policy rule will not be written to the configuration. The **save** option should be disabled only if you want to use a policy rule temporarily.
- The **default-list** option adds the rule to the default policy list. Rules are added to this list by default when the rule is created. A rule can belong to multiple policy lists. As a result, the rule remains a member of the default list even when it is subsequently assigned to additional lists.
- If the rule is going to belong to a QoS policy list for a Universal Network Profile (UNP), use the **no default-list** option when creating the rule. Doing so will give the rule precedence over default list rules when the policy list is applied to UNP device traffic.

- Note that each time a rule is assigned to a policy list, an instance of that rule is created and each instance is allocated system resources. Use the **no default-list** option with this command to exclude the rule from the default policy list.
- If the **configuration snapshot** command is entered after the **policy rule** command is configured, the resulting ASCII file will include the following additional syntax for the **policy rule** command:

  from {cli | ldap | blt}

  This syntax indicates how the rule was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in rule, this setting is not configurable.
- The **log** option is useful for determining the source of attacks on the switch firewall.
- If traps are enabled for the rule, a trap is only sent when a port disable action or UserPort shutdown operation is triggered.

Examples

```
-> policy rule rule2 condition c2 action a2
-> policy rule rule3 condition c3 action a3 no default-list
-> policy rule rule2 precedence 65535
-> policy rule rule2 validity-period vp01
-> policy rule rule2 no precedence
-> policy rule rule2 no validity-period
-> policy rule rule3 no default-list
-> no policy rule rule2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy validity-period	Configures a validity period that specifies days, times, and/or months during which an associated policy rule is in effect.
policy condition	Configures condition parameters.
policy action	Configures action parameters.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy rule	Displays information for policy rules configured on the switch.
show active policy rule	Displays only those policy rules that are currently being enforced on the switch.

MIB Objects

alaQoSRuleTable
- alaQoSRuleName
- alaQoSRuleEnabled
- alaQoSRuleSource
- alaQoSRulePrecedence
- alaQoSRuleCondition
- alaQoSRuleAction
- alaQoSRuleSave
- alaQoSRuleLog
- alaQoSRuleCountType
- alaQoSRulePacketCount
- alaQoSRuleByteCount
- alaQosRuleDefaultList

alaQoSAppliedRuleTable
- alaQoSAppliedRuleName
- alaQoSAppliedRuleEnabled
- alaQoSAppliedRuleSource
- alaQoSAppliedRulePrecedence
- alaQoSAppliedRuleCondition
- alaQoSAppliedRuleAction
- alaQoSAppliedRuleSave
- alaQoSAppliedRuleLog
- alaQoSAppliedCountType
- alaQoSAppliedPacketCount
- alaQoSAppliedByteCount
- alaQosAppliedDefaultList

policy validity-period

Configures a validity period that specifies the days and times in which a policy rule is in effect.

policy validity-period *name* **[days** *days***] [months** *months***] [hours** *hh:mm* **to** *hh:mm***] [interval** *mm:dd:yy hh:mm* **to** *mm:dd:yy hh:mm***]**

policy validity-period *name* **no {hours** | **interval}**

no policy validity-period *name*

Syntax Definitions

name	The name of the validity period (up to 31 alphanumeric characters).
days	The day(s) of the week this validity period is active. Enter the actual day of the week (e.g., **monday**, **tuesday**, **wednesday**, etc.).
months	The month(s) in which the validity period is active. Enter the actual month (e.g., **january**, **february**, **march**, etc.).
hh:mm	The time of day, specified in hours and minutes, the validity period starts and the time of day the validity period ends (e.g., 10:30 to 11:30).
mm:dd:yy hh:mm	An interval of time during which a rule is in effect. Specify a start and end to the interval period by entering a beginning date and time followed by an end date and time (e.g., 11:01:17 12:01 to 11:02:17 12:01).

Defaults

By default, no validity period is in effect for a policy rule.

parameter	default
days	no restriction
months	no restriction
hh:mm	no specific time
mm:dd:yyyy hh:mm	no interval

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a validity period from the configuration, or to remove parameters from a particular validity period. Note that at least one parameter must be associated with a validity period.
- Any combination of days, months, hours, and interval parameters is allowed. The validity period is only in effect when all specified parameters are true.

- Use the **policy rule** command to associate a validity period with a rule.
- Software and hardware resources are allocated for rules associated with a validity period even if the validity period is not active. Pre-allocating the resources makes sure the rule can be enforced when the validity period becomes active.
- If the **configuration snapshot** command is entered after the **policy validity-period** command is configured, the resulting ASCII file will include the following additional syntax for the **policy validity-period** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy validity-period vp01 days tuesday thursday months january february
-> policy validity-period vp01 hours 13:00 to 19:00
-> policy validity-period vp02 interval 01/01/05 12:01 to 02/01/05 11:59
-> policy validity-period vp01 no days thursday
-> no policy-validity period vp02
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show policy validity period	Displays information about policy validity periods.

MIB Objects

```
alaQoSValidityPeriodTable
   alaQoSValidityPeriodName
   alaQoSValidityPeriodSource
   alaQoSValidityPeriodDays
   alaQoSValidityPeriodDaysStatus
   alaQoSValidityPeriodMonths
   alaQoSValidityPeriodMonthsStatus
   alaQoSValidityPeriodHour
   alaQoSValidityPeriodHourStatus
   alaQoSValidityPeriodEndHour
   alaQoSValidityPeriodInterval
   alaQoSValidityPeriodIntervalStatus
   alaQoSValidityPeriodEndInterval
alaQoSAppliedValidityPeriodTable
   alaQoSAppliedValidityPeriodName
   alaQoSAppliedValidityPeriodSource
   alaQoSAppliedValidityPeriodDays
   alaQoSAppliedValidityPeriodDaysStatus
   alaQoSAppliedValidityPeriodMonths
   alaQoSAppliedValidityPeriodMonthsStatus
   alaQoSAppliedValidityPeriodHour
   alaQoSAppliedValidityPeriodHourStatus
   alaQoSAppliedValidityPeriodEndHour
   alaQoSAppliedValidityPeriodInterval
   alaQoSAppliedValidityPeriodIntervalStatus
   alaQoSAppliedValidityPeriodEndInterval
```

policy list

Configures a QoS policy list. There are four types of lists available: a Universal Network Profile (UNP) policy list, an egress policy list, an Application Fingerprinting policy list, and a default policy list.

policy list *list_name* **type {unp | egress | appfp | empacl} [enable | disable]**

no policy list *list_name*

Syntax Definitions

list_name	The name to assign to the policy list. Note that the list name is case sensitive.
unp	Applies the list of policy rules to traffic classified into the User Network Profile to which the list is assigned
egress	Applies the list of policy rules to traffic egressing on switch ports. *This parameter is not supported on the OmniSwitch 6465 or OmniSwitch 6560.*
appfp	Applies the list of policy rules to an Application Fingerprinting interface. *This parameter is supported only on the OmniSwitch 6900.*
empacl	*This parameter is not supported.*
enable	Enables the policy list.
disable	Disables the policy list.

Defaults

A default policy list is available when the switch boots up; all policy rules belong to this list unless otherwise specified (see the **policy list rules** and **policy rule** commands for more information).

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a policy list from the configuration.
- Once a policy list is created, use the **policy list rules** command to add rules to the list.
- Any policy list configured through this command is not active on the switch until the **qos apply** command is issued.
- If the **configuration snapshot** command is entered after the **policy list** command is configured, the resulting ASCII file will include the following additional syntax for the **policy list** command:

  from {cli | ldap | blt}

This syntax indicates how the list was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy list unp1 type unp
-> policy list unp1 disable
-> policy list unp1 enable
-> no policy list unp1
```

Release History

Release 7.2.1; command was introduced.
Release 8.4.1; **egress** parameter added.

Related Commands

policy list rules	Assigns QoS policy rules to a QoS policy list.
policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show policy rule	Displays information for policy rules configured on the switch.
show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy list	Displays information for policy lists configured on the switch.

MIB Objects

```
alaQoSRuleGroupsTable
   alaQoSRuleDefaultList
   alaQoSRuleGroupsName
   alaQosRuleGroupsSource
   alaQosRuleGroupsType
   alaQosRuleGroupsEnabled
   alaQosRuleGroupsStatus
alaQosAppliedRuleGroupsTable
   alaQosAppliedRuleGroupsName
   alaQosAppliedRuleGroupsSource
   alaQosAppliedGroupsType
   alaQosAppliedGroupsEnabled
   alaQosAppliedRuleGroupsStatus
```

policy list rules

Assigns existing QoS policy rules to the specified QoS policy list.

policy list *list_name* **rules** *rule_name* **[***rule_name2***...]**

policy list *list_name* **no rules** *rule_name* **[***rule_name2***...]**

Syntax Definitions

list_name	The name of an existing QoS policy list. Note that the list name is case sensitive.
rule_name	The name of an existing QoS policy rule to include in the policy list.
rule_name2	Optional. The name of another QoS policy rule to include in the policy list. Separate each rule name specified with a space.

Defaults

A default policy list is available when the switch boots up. This list has no name and is not configurable. All QoS policy rules are assigned to the default list unless the **no default-list** option of the **policy rule** command is used.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a policy rule from an existing list.
- The QoS policy list and rule names specified with this command must already exist in the switch configuration.
- A rule may belong to a Universal Network Profile (UNP) list, the default list, and an egress policy list at the same time. By default, a rule is assigned to a default policy list when the rule is created. If the rule is subsequently assigned to another policy list, it still remains associated with the default list.
- If a rule is a member of multiple policy lists but one or more of these lists are disabled, the rule is still active in those lists that are enabled.
- If the QoS status of a policy rule is disabled, then the rule is disabled for all lists even if a list to which the policy rule belongs is enabled.
- If a policy rule is going to be assigned to a UNP policy list, make sure the rule was created using the **no default-list** option of the **policy rule** command. This will ensure that the rule will take precedence over other default list rules when the UNP policy list is applied to device traffic.
- A QoS policy list that is assigned to an Application Fingerprinting interface must contain policy rules with the **appfp-group** condition.
- Only those rules that are assigned to an egress policy list are applied to egress traffic. When configuring egress policy lists, consider the following:

  - Egress policy lists are not supported on the OmniSwitch 6465 or OmniSwitch 6560.
  - Only one egress policy list per switch is supported, to which IPv4 and IPv6 rules can be added.
  - Applying egress policy lists to SPB or VXLAN SAP ports is not supported.
  - Only the following policy conditions and actions are supported when creating rules for an egress policy list:

policy conditions	policy actions
Destination port Destination VLAN Source IPv4 address Source IPv6 address IPv6 (qualifier for traffic types)	Disposition (drop/accept)

- Using policy lists that contain rules with a source port condition are not supported when applied to 10G ports on an OmniSwitch 6560.
- On the OmniSwitch 6465, policy rules containing the following conditions are not supported in a UNP policy list:
  - Source port group
  - Source IPv6 address
  - IPv6 flow label
- On the OmniSwitch 6560 and OmniSwitch 9900, only policy rules with the following conditions can be assigned to a UNP policy list:
  - Destination MAC
  - EtherType
  - Source VLAN
  - SIP
  - DIP / DIPv6
  - Layer 4 Protocol
  - Layer 4 source port
  - Layer 4 destination port
  - Source port
- Any policy list configured through this command is not active on the switch until the **qos apply** command is issued.

Examples

```
-> policy list unp1 rules r1 r2 r3
-> policy list unp1 no rules r2
```

Release History

Release 7.2.1; command was introduced.

Related Commands

policy list	Configures a QoS policy list.
policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show policy rule	Displays information for policy rules configured on the switch.
show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy list	Displays information for policy lists configured on the switch.

MIB Objects

```
alaQoSRuleGroupsTable
   alaQoSRuleDefaultList
   alaQoSRuleGroupsName
   alaQosRuleGroupsSource
   alaQosRuleGroupsType
   alaQosRuleGroupsEnabled
   alaQosRuleGroupsStatus
alaQosAppliedRuleGroupsTable
   alaQosAppliedRuleGroupsName
   alaQosAppliedRuleGroupsSource
   alaQosAppliedGroupsType
   alaQosAppliedGroupsEnabled
   alaQosAppliedRuleGroupsStatus
```

policy network group

Configures a network group name and its associated IP addresses. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the network group.

policy network group *net_group ip_address* **[mask** *net_mask***] [***ip_address2* **[mask** *net_mask2***]...]**

no policy network group *net_group*

policy network group *net_group* **no** *ip_address* **[mask** *netmask***] [***ip_address2* **[mask** *net_mask2***]...]**

Syntax Definitions

net_group	The name of the network group (up to 31 alphanumeric characters).
ip_address	An IPv4 or IPv6 address included in the network group.
net_mask	The mask for the IPv4 or IPv6 address. If no mask is entered, the address is assumed to be a host address.
ip_address2	Optional. Another IPv4 or IPv6 address to be included in the network group. Multiple IP addresses may be configured for a network group. Separate each address/mask combination with a space.
net_mask2	Optional mask for the IPv4 or IPv6 address. If no mask is entered, the natural mask for the address will be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to configure a group of IP addresses to which you want to apply QoS rules. Rather than create a condition for each IP address, group the addresses together. Use the **policy condition** command to associate a condition with the network group.
- Use the **no** form of the command to remove a network group from the configuration, or to remove an IP address from a network group.
- If the **configuration snapshot** command is entered after the **policy network group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy network group** command:

  from {cli | ldap | blt}

  This syntax indicates how the network group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in network group, this setting is not configurable.

Examples

```
-> policy network group webgroup1 10.10.12.5 10.50.3.1
-> policy network group webgroup1 no 10.10.12.5
-> no policy network group webgroup1

-> policy network group webgroup2 2001:db8:4132:86::19a 2002:c633:6489::35
-> policy network group webgroup2 no 2002:c633:6489::35
-> no policy network group webgroup2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A network group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy network group	Displays information for policy network groups.

MIB Objects

```
alaQoSNetworkGroupsTable
   alaQoSNetworkGroupsName
   alaQoSNetworkGroupsSource
alaQoSAppliedNetworkGroupsTable
   alaQoSAppliedNetworkGroupsName
   alaQoSAppliedNetworkGroupsSource
alaQoSNetworkGroupTable
   alaQoSNetworkGroupIpAddr
   alaQoSNetworkGroupsIpMask
alaQoSAppliedNetworkGroupTable
   alaQoSAppliedNetworkGroupIpAddr
   alaQoSAppliedNetworkGroupsIpMask
```

policy service group

Configures a service group and its associated services. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the service group.

policy service group *service_group service_name1* **[***service_name2...***]**

no policy service group *service_group*

policy service group *service_group* **no** *service_name1* **[***service_name2...***]**

Syntax Definitions

service_group	The name of the service group (up to 31 alphanumeric characters).
service_name1	The service name is configured through the **policy service** command and includes information about protocol, source port, and destination port.
service_name2...	Optional. Additional service names may be configured for a service group. Separate each service name with a space.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to configure a group of services to which you want to apply QoS rules. Rather than create a condition for each service, group services together. Use the **policy condition** command to associate a condition with the service group.
- Use the **no** form of the command to remove a service group from the configuration, or to remove a service from a service group.
- To drop packets destined to specific TCP and UDP ports, create port services for the traffic that you want dropped and add these services to a service group. Then create a condition for this service group and a source port group, which can then be used in a deny rule. Refer to the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about ACL security enhancements.
- If the **configuration snapshot** command is entered after the **policy service group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service group** command:

  from {cli | ldap | blt}

  This syntax indicates how the service group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in service group, this setting is not configurable.

Examples

```
-> policy service group servgroup2 telnet ftp
-> policy service group servgroup2 no telnet
-> no policy service group servgroup2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy service	Configures a service that may be used as part of a policy service group.
policy condition	Configures a policy condition. A network group may be configured as part of a policy condition.
show policy service group	Displays information for policy service groups.

MIB Objects

```
alaQoSServiceGroupsTable
   alaQoSServiceGroupsName
   alaQoSServiceGroupsSource
alaQoSAppliedServiceGroupsTable
   alaQoSAppliedServiceGroupsName
   alaQoSAppliedServiceGroupsSource
alaQoSServiceGroupTable
   alaQoSServiceGroupServiceName
alaQoSAppliedServiceGroupTable
   alaQoSAppliedServiceGroupServiceName
```

policy mac group

Configures a MAC group and its associated MAC addresses. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the MAC group.

policy mac group *mac_group mac_address* **[mask** *mac_mask***] [***mac_address2* **[mask** *mac_mask2***]...]**

no policy mac group *mac_group*

policy mac group *mac_group* **no** *mac_address* **[mask** *mac_mask***] [***mac_address2* **[mask** *mac_mask2***]...]**

Syntax Definitions

mac_group	The name of the MAC group (up to 31 alphanumeric characters).
mac_address	The MAC address associated with the group (for example, 00:20:da:05:f6:23).
mac_mask	The mask of the MAC address, used to identify which bytes in the MAC address are significant when comparing the MAC address in the received frame with the MAC address in the policy condition. If no mask is specified, the switch automatically uses ff:ff:ff:ff:ff:ff.
mac_address2	Optional. Additional MAC addresses may be configured for a MAC group. Separate each address with a space.
mac_mask2	The mask of an additional MAC address, used to identify which bytes in the MAC address are significant when comparing the MAC address in the received frame with the MAC address in the policy condition. If no mask is specified, the switch automatically uses ff:ff:ff:ff:ff:ff.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to configure a group of source or destination MAC addresses to which you want to apply QoS rules. Rather than create a condition for each MAC address, group MAC addresses together. Use the **policy condition** command to associate a condition with the MAC group.
- Use the **no** form of the command to remove a MAC group from the configuration, or to remove a MAC address from a MAC group.
- The MAC group name “alaPhones” is a reserved group name used to identify the MAC addresses of IP phones. See the **qos phones** command for more information.
- If the **configuration snapshot** command is entered after the **policy map group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy map group** command:

from {cli | ldap | blt}

This syntax indicates how the map group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy mac group mac_group1 00:20:da:05:f6:23 00:20:da:05:f6:24
-> no policy mac group mac_group1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A MAC group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy mac group	Displays information about policy MAC groups.

MIB Objects

```
alaQoSMACGroupsTable
   alaQoSMACGroupsName
   alaQoSMACGroupsSource
alaQoSAppliedMACGroupsTable
   alaQoSAppliedMACGroupsName
   alaQoSAppliedMACGroupsSource
alaQoSMACGroupTable
   alaQoSMACGroupMacAddr
   alaQoSMACGroupMacMask
alaQoSAppliedMACGroupTable
   alaQoSAppliedMACGroupMacAddr
   alaQoSAppliedMACGroupMacMask
```

policy port group

Configures a port group and its associated slot and port numbers. A port group may be attached to a policy condition. The action associated with that policy will be applied to all members of the port group.

policy port group *group_name* **{***chassis//slot/port***[-***port2***]** | *agg_id***[-***agg_id2***]} [***chassis//slot/port***[-***port2***]** | *agg_id***[-***agg_id2***]]**

no policy port group *group_name*

policy port group *group_name* **no {***chassis//slot/port***[-***port2***]** | *agg_id***[-***agg_id2***]} [***chassis//slot/port***[-***port2***]** | *agg_id***[-***agg_id2***]]**

Syntax Definitions

group_name	The name of the port group (up to 31 alphanumeric characters).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port (or port range) to be included in the group. At least one slot/port combination must be specified. Additional combinations may be included in the group; each combination should be separated by a space.
*agg_id***[-***agg_id2***]**	A link aggregate ID to be included in the group. Use a hyphen to specify a range of IDs (10-15). Additional combinations may be included in the group; each combination should be separated by a space. *This parameter is not supported on the OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 9900.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to configure a group of ports or link aggregates to which you want to apply QoS rules. Rather than create a condition for each port, group ports together. Use the **policy condition** command to associate a condition with the port group.
- Configuring ports and link aggregates in the same port group is allowed.
- Adding link aggregate member ports to a QoS port group is not recommended; doing so may cause undesired results when the port group is used in a QoS policy, particularly if only a subset of member ports is added to the port group.
- Use the **no** form of the command to remove a port group from the configuration, or to remove a slot/port from a port group.
- If a range of ports is specified using the syntax *chassis/slot/port-port2* (that is, 1/2/1-8), a single port within that range cannot be removed on its own. The entire range must be deleted as it was entered.

- If a range of link aggregates is specified using the syntax *agg_id***[**-*agg_id2* (that is, 10-15), a single aggregate within that range cannot be removed on its own. The entire range must be deleted as it was entered.
- When a port group is used as part of a policy rule and a policy action specifies a maximum bandwidth, each interface in the port group will be allowed the maximum bandwidth.
- To prevent IP source address spoofing, add ports to the port group called **UserPorts**. This port group does not need to be used in a condition or rule to be effected on flows and applies to both bridged and routed traffic. Ports added to the UserPorts group will block spoofed traffic while still allowing normal traffic on the port. Refer to the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about ACL security enhancements.
- Adding ports to the **UserPorts** group is not supported on the OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 9900.
- Use the **qos user-port** command to configure the option to filter or administratively disable a port when a specific type of traffic (Spoof, RIP, BPDU, OSPF, and/or BGP) is received on a port that is a member of the pre-defined UserPorts group.
- If the **configuration snapshot** command is entered after the **policy port group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy port group** command:

  from {cli | ldap | blt}

  This syntax indicates how the port group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy port group port_group4 3/1/1-2 4/3/1 5/4/1
-> policy port group port_group4 no 3/1/1-2
-> policy port group UserPorts 4/1/1-8 5/1/1-8
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; *agg_id* parameter added.

Related Commands

policy condition	Configures a policy condition. A port group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
policy action maximum bandwidth	Configures a maximum bandwidth value for a policy action.
show policy port group	Displays information about policy port groups.

MIB Objects

```
alaQoSPortGroupsTable
   alaQoSPortGroupsName
   alaQoSPortGroupSlot
   alaQoSPortGroupPort
   alaQoSPortGroupPortEnd
alaQoSAppliedPortGroupsTable
   alaQoSAppliedPortGroupsName
   alaQoSAppliedPortGroupSlot
   alaQoSAppliedPortGroupPort
   alaQoSAppliedPortGroupPortEnd
```

policy map group

Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values. A map group may be referenced in a policy action with the **map** keyword.

policy map group *map_group* **{***value1***:***value2***...}**

no policy map group *map_group*

policy map group no {*value1***:***value2***...}**

Syntax Definitions

map_group	The name of the map group (up to 31 alphanumeric characters).
value1	The 802.1p, ToS, or DSCP value to be mapped to another value. May be a value or a range of values (for example, **1-2**).
value2...	The 802.1p, ToS, or DSCP value to be used in place of *value1*. Additional mapping pairs may be included.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a mapping pair or to remove the map group entirely.
- The map group may contain more than one mapping pair.
- If the **configuration snapshot** command is entered after the **policy map group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy map group** command:

  from {cli | ldap | blt}

  This syntax indicates how the map group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy map group tosGroup 1-4:3 5-6:5 7:6
-> policy map group tosGroup no 7:6
-> no policy map group tosGroup
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy action map	Configures a mapping group for a policy action.

MIB Objects

```
alaQoSMapGroupsTable
   alaQoSMapGroupsName
   alaQoSMapGroupsSource
alaQoSAppliedMapGroupsTable
   alaQoSAppliedMapGroupsName
   alaQoSAppliedMapGroupsSource
alaQoSMapGroupTable
   alaQoSMapGroupKey
   alaQoSMapGroupKeyEnd
   alaQoSMapGroupValue
alaQoSAppliedMapGroupTable
   alaQoSAppliedMapGroupKey
   alaQoSAppliedMapGroupKeyEnd
   alaQoSAppliedMapGroupValue
```

policy service

Configures a service that may be used as part of a policy service group or included as part of a policy condition. A service is a source and/or destination TCP or UDP port or port range.

This overview section describes the base command. *At least one option must be configured with the base command.* Some options may be used in combination; some options are shortcuts for keyword combinations (see the Usage Guidelines). Options are described as separate commands. See the command descriptions and usage guidelines for valid combinations.

Use the **no** form for keywords to remove a parameter from a service.

policy service *service_name*
[protocol *protocol***]**
[source ip-port *port***[-***port***]]**
[destination ip-port *port***[-***port***]]**
[source tcp-port *port***[-***port***]]**
[destination tcp-port *port***[-***port***]]**
[source udp-port *port***[-***port***]]**
[destination udp-port *port***[-***port***]]**

no policy service *service_name*

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
protocol	The protocol associated with the service. The range of values is 0–255. Currently a value of 6 (for TCP) or 17 (for UDP) is supported. This value must be specified for **source ip-port** or **destination ip-port**; it cannot be specified for **source tcp-port**, **destination tcp-port**, **source udp-port**, or **destination udp-port**.
port	The well-known port number (or port range) for the desired service. For example, the port number for Telnet is 23. Specify a range of ports using a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.

- The command options offer alternate ways of configuring TCP or UDP ports for a service. Note that port types (TCP or UDP) cannot be mixed in the same service. The following table shows how the keywords are used:

To configure:	Use keywords:	Notes
TCP or UDP ports for a service	**protocol** **source ip-port** **destination ip-port**	*The protocol must be specified with at least one source or destination port.*
TCP ports for a service	**source tcp-port** **destination tcp-port**	*Keywords may be used in combination.*
UDP ports for a service	**source udp-port** **destination udp-port**	*Keywords may be used in combination.*

- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

The following two commands show two different ways of configuring the same service:

```
-> policy service telnet2 protocol 6 destination ip-port 23
-> policy service telnet3 destination tcp-port 23
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

alaQoSServiceTable

- alaQoSServiceName
- alaQoSServiceSource
- alaQoSServiceIpProtocol
- alaQoSServiceSourceIpPort
- alaQoSServiceSourceIpPortEnd
- alaQoSServiceDestinationIpPort
- alaQoSServiceDestinationIpPortEnd
- alaQoSServiceSourceTcpPort
- alaQoSServiceSourceTcpPortEnd
- alaQoSServiceDestinationTcpPort
- alaQoSServiceDestinationTcpPortEnd
- alaQoSServiceSourceUdpPort
- alaQoSServiceSourceUdpPortEnd
- alaQoSServiceDestinationUdpPort
- alaQoSServiceDestinationUdpPortEnd

alaQoSAppliedServiceTable

- alaQoSAppliedServiceName
- alaQoSAppliedServiceSource
- alaQoSAppliedServiceIpProtocol
- alaQoSAppliedSourceIpPort
- alaQoSAppliedSourceIpPortEnd
- alaQoSAppliedServiceDestinationIpPort
- alaQoSAppliedServiceDestinationIpPortEnd
- alaQoSAppliedSourceTcpPort
- alaQoSAppliedSourceTcpPortEnd
- alaQoSAppliedServiceDestinationTcpPort
- alaQoSAppliedServiceDestinationTcpPortEnd
- alaQoSAppliedSourceUdpPort
- alaQoSAppliedSourceUdpPortEnd
- alaQoSAppliedServiceDestinationUdpPort
- alaQoSAppliedServiceDestinationUdpPortEnd

policy service protocol

Configures a service with a protocol and IP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **protocol** *protocol* **{[source ip-port** *port***[-***port***]] [destination ip-port** *port***[-***port***]]}**

no policy service *service_name*

policy service *service_name* **no {source ip-port | destination ip-port}**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
protocol	The protocol associated with the service. The range of values is 0–255. Currently a value of 6 (for TCP) or 17 (for UDP) is supported.
port	The well-known port number (or port range) for the desired service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a service from the configuration or to remove parameters from a particular service. (A protocol value cannot be removed from a service.)
- Shortcut commands for the **policy service protocol** command include the following: **policy service source tcp-port**, **policy service destination tcp-port**, **policy service source udp-port**, and **policy service destination udp-port**.
- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service telnet2 protocol 6 destination ip-port 23 source ip-port 22
-> policy service telnet2 no source ip-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceIpProtocol
   alaQoSServiceSourceIpPort
   alaQoSServiceSourceIpPortEnd
   alaQoSServiceDestinationIpPort
   alaQoSServiceDestinationIpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceIpProtocol
   alaQoSAppliedSourceIpPort
   alaQoSAppliedSourceIpPortEnd
   alaQoSAppliedServiceDestinationIpPort
   alaQoSAppliedServiceDestinationIpPortEnd
```

policy service source tcp-port

Configures a service with a source TCP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **source tcp-port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no source tcp-port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired TCP service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.
- Ports associated with a particular service must all be of the same type. (The **destination tcp-port** keyword may be used with this command; other keywords for the command are not allowed.)
- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service serv_5 source tcp-port 21-22
-> policy service serv_5 no source tcp-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceSourceTcpPort
   alaQoSServiceSourceTcpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedSourceTcpPort
   alaQoSAppliedSourceTcpPortEnd
```

policy service destination tcp-port

Configures a service with a destination TCP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **destination tcp-port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no destination tcp-port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired TCP service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a service from the configuration, or to remove parameters from a particular service.
- This command is a shortcut for the **policy service protocol** command.
- A policy service may be grouped in a policy group using the **policy service group** command. A policy condition may then be associated with the service group.
- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service service4 destination tcp-port 23
-> policy service service4 no destination tcp-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceDestinationTcpPort
   alaQoSServiceDestinationTcpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceDestinationTcpPort
   alaQoSAppliedServiceDestinationTcpPortEnd
```

policy service source udp-port

Configures a service with a source UDP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **source udp-port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no source udp-port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired UDP service. Specify a port range with a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.
- Ports associated with a particular service must all be of the same type. (The **destination tcp-port** keyword may be used with this command; other keywords for the command are not allowed.)
- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service serv_a source udp-port 1000
-> no policy service serv_a source udp-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceSourceUdpPort
   alaQoSServiceSourceUdpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedSourceUdpPort
   alaQoSAppliedSourceUdpPortEnd
```

policy service destination udp-port

Configures a service with a destination UDP port or port range that may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **destination udp-port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no destination udp-port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired UDP service. For example, a port number for NETBIOS is 137. A port range should be separated by a hyphen (for example, **137-138**).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- A policy service may be grouped in a policy group using the **policy service group** command. A policy condition may then be associated with the service group.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service.
- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service service4 destination udp-port 137
-> policy service service4 no destination udp-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group	Configures a policy service group, which is made up of policy services.
policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy service	Displays information about policy services configured on the switch.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceDestinationUdpPort
   alaQoSServiceDestinationUdpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceDestinationUdpPort
   alaQoSAppliedServiceDestinationUdpPortEnd
```

policy condition

Creates a QoS policy condition. The condition determines what parameters the switch uses to classify incoming flows. Condition parameters may be configured when the condition is created; or parameters may be configured for an existing condition. At least one parameter must be configured for a condition.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the **no** form for keywords to remove a parameter from the condition.

Some condition parameters may not be supported depending on the platform you are using. Also some condition parameters may not be supported with some action parameters. See the condition/action tables in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

policy condition *condition_name*
[source ip *ip_address* **[mask** *netmask***]]**
[source ipv6 {any | *ipv6_address* **[mask** *netmask***]}**
[destination ip *ip_address* **[mask** *netmask***]]**
[destination ipv6 {any | *ipv6_address* **[mask** *netmask***]}**
[multicast ip *ip_address* **[mask** *netmask***]]**
[source network group *network_group***]**
[destination network group *network_group***]**
[multicast network group *multicast_group***]**
[source ip-port *port***[-***port***]]**
[destination ip-port *port***[-***port***]]**
[source tcp-port *port***[-***port***]]**
[destination tcp-port *port***[-***port***]]**
[source udp-port *port***[-***port***]]**
[destination udp-port *port***[-***port***]]**
[ethertype *etype***]**
[established]
[tcpflags {any | all} *flag* **[mask** *flag***]**
[service *service***]**
[service group *service_group***]**
[icmptype *type***]**
[icmpcode *code***]**
[ip-rotocol *protocol***]**
[ipv6]
[flow-label *flow_label_value***]**
[tos *tos_value tos_mask***]**
[dscp {*dscp_value***[-***value***} [***dscp_mask***]]**
[source mac *mac_address* **[mask** *mac_mask***]]**
[destination mac *mac_address* **[mask** *mac_mask***]]**
[source mac group *group_name***]**
[destination mac group *mac_group***]**
[source vlan *vlan_id***]**
[destination vlan *vlan_id***]**
[802.1p *802.1p_value***]**
[source port *chassis/slot/port***[-***port2***]]**

[source port group *group_name***}**
[destination port *chassis/slot/port***[-***port2***]]**
[destination port group *group_name***]**
[vrf {*vrf_name* | **default}]**
[fragments]
[appfp-group *group_name***]**

no policy condition *condition_name*

Syntax Definitions

condition_name	The name of the condition. Any alphanumeric string.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- A policy condition and a policy action are combined to make a policy rule. See the **policy rule** command.
- Use the **qos apply** command to activate configuration changes.
- If multiple keywords are defined for a single condition, the traffic flow must match all of the parameters in the condition before the rule is enforced.
- Use the **no** form of the command to remove a condition from a policy rule.
- At least one parameter must be associated with a condition.
- If the **configuration snapshot** command is entered after the **policy condition** command is configured, the resulting ASCII file will include the following additional syntax for the **policy condition** command:

  from {cli | ldap | blt}

  This syntax indicates how the condition was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in condition, this option is not configurable.

Examples

```
-> policy condition cond4 source port 3/1/1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Configures a policy action.
policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSource
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSource
```

policy condition source ip

Configures a source IP address for a policy condition.

policy condition *condition_name* **source ip** *ip_address* **[mask** *netmask***]**

policy condition *condition_name* **no source ip**

Syntax Definitions

condition_name	The name of the condition.
ip_address	The source IP address of the Layer 3 flow.
netmask	The mask for the source IP address.

Defaults

parameter	default
netmask	IP address class

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A source IP address and a source IP network group cannot be specified in the same condition.
- Use the **no** form of the command to remove a source IP address from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond3 source ip 173.201.18.3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about a particular policy condition configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceIpAddr
   alaQoSConditionSourceIpMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceIpAddr
   alaQoSAppliedConditionSourceIpMask
```

policy condition source ipv6

Configures a source IPv6 address for a policy condition.

policy condition *condition_name* **source ipv6 {any |** *ipv6_address* **[mask** *netmask***]}**

policy condition *condition_name* **no source ipv6**

Syntax Definitions

condition_name	The name of the condition.
any	Any source IPv6 address.
ipv6_address	A specific source IPv6 address.
netmask	The mask for the source IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a source IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- If a mask is not specified, the IPv6 address is assumed to be a host address.
- On the OmniSwitch 6560 and OmniSwitch 9900, a source IPv6 address policy condition is supported only for *egress* IPv6 ACLs.

Examples

```
-> policy condition cond3 source ipv6 ::1234:531F:BCD2:F34A
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about a particular policy condition configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceIpv6Addr
   alaQoSConditionSourceIpv6AddrStatus
   alaQoSConditionSourceIpv6Mask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceIpv6Addr
   alaQoSAppliedConditionSourceIpv6AddrStatus
   alaQoSAppliedConditionSourceIpMask
```

policy condition destination ip

Configures a destination IP address for a policy condition.

policy condition *condition_name* **destination ip** *ip_address* **[mask** *netmask***]**

policy condition *condition_name* **no destination ip**

Syntax Definitions

condition_name	The name of the condition.
ip_address	The source IP address of the Layer 3 flow.
netmask	The mask for the source IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A destination IP address and a destination IP network group cannot be specified in the same condition.
- Use the **no** form of the command to remove a destination IP address from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 destination ip 208.192.21.0 mask 255.255.255.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about a particular policy condition configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationIpAddr
   alaQoSConditionDestinationIpMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationIpAddr
   alaQoSAppliedConditionDestinationIpMask
```

policy condition destination ipv6

Configures a destination IPv6 address for a policy condition.

policy condition *condition_name* **destination ipv6 {any |** *ipv6_address* **[mask** *netmask***]}**

policy condition *condition_name* **no destination ipv6**

Syntax Definitions

condition_name	The name of the condition.
any	Any destination IPv6 address.
ipv6_address	A specific destination IPv6 address.
netmask	The mask for the destination IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a destination IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- If a mask is not specified, the IPv6 address is assumed to be a host address.
- On the OmniSwitch 6560 and OmniSwitch 9900, a destination IPv6 address policy condition is supported only for *ingress* IPv6 ACLs.

Examples

```
-> policy condition cond3 destination ipv6 ::1234:531f:bcd2:f34a
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about a particular policy condition configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationIpv6Addr
   alaQoSConditionDestinationIpv6AddrStatus
   alaQoSConditionDestinationIpv6Mask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationIpv6Addr
   alaQoSAppliedConditionDestinationIpv6AddrStatus
   alaQoSAppliedConditionDestinationIpMask
```

policy condition multicast ip

Configures a multicast IP address for a policy condition.

policy condition *condition_name* **multicast ip** *ip_address* **[mask** *netmask***]**

policy condition *condition_name* **no multicast ip**

Syntax Definitions

condition_name	The name of the condition.
ip_address	The multicast IP address.
netmask	Optional. The mask for the multicast IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A multicast IP address and a multicast network group cannot be specified in the same condition.
- Use the **no** form of the command to remove a multicast IP address from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 multicast ip 224.1.1.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSMulticastIpAddr
   alaQoSMulticastIpMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedMulticastIpAddr
   alaQoSAppliedMulticastIpMask
```

policy condition source network group

Associates a source network group with a policy condition.

policy condition *condition_name* **source network group** *network_group*

policy condition *condition_name* **no source network group**

Syntax Definitions

condition_name	The name of the condition.
network_group	The name of the source network group. Network groups are configured through the **policy network group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a source network group from a condition; however, at least one classification parameter must be associated with a condition.
- A source IP address and a source IP network group cannot be specified in the same condition.
- On the OmniSwitch 6560 and OmniSwitch 9900, a source network group policy condition with an IPv6 address (includes user-configured and the built-in “Switch6” group) is supported only for *egress* IPv6 ACLs,

Examples

```
-> policy condition cond5 source network group webgroup1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy network group	Configures a network group name and its associated IP addresses.
show policy condition	Shows information about policy conditions configured on the switch.
show policy network group	Displays information about policy network groups.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceNetworkGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceNetworkGroup
```

policy condition destination network group

Associates a destination network group with a policy condition.

policy condition *condition_name* **destination network group** *network_group*

policy condition *condition_name* **no destination network group**

Syntax Definitions

condition_name	The name of the condition.
network_group	The name of the destination network group. Network groups are configured through the **policy network group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a destination network group from a condition; however, at least one classification parameter must be associated with a condition.
- A destination IP address and a destination IP network group cannot be specified in the same condition.
- On the OmniSwitch 6560 and OmniSwitch 9900, a destination network group policy condition with an IPv6 address is supported only for *ingress* IPv6 ACLs,

Examples

```
-> policy condition cond6 destination network group webgroup1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
policy network group	Configures a network group name and its associated IP addresses.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.
show policy network group	Displays information about policy network groups.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationNetworkGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationNetworkGroup
```

policy condition multicast network group

Associates a multicast group with a policy condition.

policy condition *condition_name* **multicast network group** *multicast_group*

policy condition *condition_name* **no multicast network group**

Syntax Definitions

condition_name	The name of the condition.
multicast_group	The multicast group name. Multicast groups are configured through the **policy network group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a multicast group from a condition; however, at least one classification parameter must be associated with a condition.
- A multicast address and a multicast network group cannot be specified in the same condition.

Examples

```
-> policy condition cond3 multicast group video2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy network group	Configures a network group name and its associated IP addresses.
show policy condition	Shows information about policy conditions configured on the switch.
show policy network group	Displays information about policy network groups.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionMulticastNetworkGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionMulticastNetworkGroup
```

policy condition source ip-port

Configures a source IP port number for a policy condition.

policy condition *condition_name* **source ip-port** *port***[-***port***]**

policy condition *condition_name* **no source ip-port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP or UDP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a source IP port from a condition; however, at least one classification parameter must be associated with a condition.
- The protocol (TCP or UDP) must be specified in the condition, either on the same command line or in a previous command. Use the **ip-protocol** keyword. See the **policy condition ip-protocol** command.
- The same condition cannot specify a source IP port with a source TCP port, source UDP port, service, or service group.

Examples

```
-> policy condition cond1 ip-protocol 6 source ip-port 137
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition ip-protocol	Configures an IP protocol for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceIpPort
   alaQoSConditionSourceIpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceIpPort
   alaQoSAppliedConditionSourceIpPortEnd
```

policy condition destination ip-port

Configures a destination IP port number for a policy condition.

policy condition *condition_name* **destination ip-port** *port***[-***port***]**

policy condition *condition_name* **no destination ip-port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP or UDP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a destination IP port from a condition; however, at least one classification parameter must be associated with a condition.
- The protocol (TCP or UDP) must be specified in the same condition, either on the same command line or in a previous command. Use the **ip-protocol** keyword. See the **policy condition ip-protocol** command.
- The same condition cannot specify a destination IP port with a service or service group.

Examples

```
-> policy condition cond2 ip-protocol 6 destination ip-port 137-138
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition ip-protocol	Configures an IP protocol for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationIpPort
   alaQoSConditionDestinationIpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationIpPort
   alaQoSAppliedConditionDestinationIpPortEnd
```

policy condition source tcp-port

Configures a source TCP port number for a policy condition.

policy condition *condition_name* **source tcp-port** *port***[-***port***]**

policy condition *condition_name* **no source tcp-port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a source TCP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the **policy condition source ip-port** command, which requires that the protocol also be specified. Rather than specifying **source ip-port** and **ip-protocol**, use **source tcp-port**.
- The same condition cannot specify a source TCP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.
- Use this condition in combination with the IPv6 condition (**policy condition ipv6**) to configure IPv6 policies for Layer 4 information, services, and service groups.

Examples

```
-> policy condition cond3 source tcp-port 137
-> policy condition cond4 ipv6 source tcp-port 21
-> policy condition cond3 no source tcp-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition ip-protocol	Configures an IP protocol for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceTcpPort
   alaQoSConditionSourceTcpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceTcpPort
   alaQoSAppliedConditionSourceTcpPortEnd
```

policy condition destination tcp-port

Configures a destination TCP port number for a policy condition.

policy condition *condition_name* **destination tcp-port** *port***[-***port***]**

policy condition *condition_name* **no destination tcp-port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a destination TCP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the **policy condition destination ip-port** command, which requires that the protocol also be specified. Rather than specifying **destination ip-port** and **ip-protocol**, use **destination tcp-port**.
- The same condition cannot specify a destination TCP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.
- Use this condition in combination with the IPv6 condition (**policy condition ipv6**) to configure IPv6 policies for Layer 4 information, services, and service groups.

Examples

```
-> policy condition cond4 destination tcp-port 137-138
-> policy condition cond5 ipv6 destination tcp-port 140
-> policy condition cond4 no destination tcp-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition ip-protocol	Configures an IP protocol for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationTcpPort
   alaQoSConditionDestinationTcpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationTcpPort
   alaQoSAppliedConditionDestinationTcpPortEnd
```

policy condition source udp-port

Configures a source UDP port number for a policy condition.

policy condition *condition_name* **source udp-port** *port***[-***port***]**

policy condition *condition_name* **no source udp-port**

Syntax Definitions

condition_name	The name of the condition.
port	The UDP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a source UDP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the **policy condition source ip-port** command, which requires that the protocol also be specified. Rather than specifying **source ip-port** and **ip-protocol**, use **source udp-port**.
- The same condition cannot specify a source UDP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.
- Use this condition in combination with the IPv6 condition (**policy condition ipv6**) to configure IPv6 policies for Layer 4 information, services, and service groups.

Examples

```
-> policy condition cond5 source udp-port 1200-1400
-> policy condition cond6 ipv6 source udp-port 1000
-> policy condition cond5 no source udp-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition ip-protocol	Configures an IP protocol for a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceUdpPort
   alaQoSConditionSourceUdpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceUdpPort
   alaQoSAppliedConditionSourceUdpPortEnd
```

policy condition destination udp-port

Configures a destination UDP port number for a policy condition.

policy condition *condition_name* **destination udp-port** *port***[-***port***]**

policy condition *condition_name* **no destination udp-port**

Syntax Definitions

condition_name	The name of the condition.
port	The UDP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a destination UDP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the **policy condition destination ip-port** command, which requires that the protocol also be specified. Rather than specifying **destination ip-port** and **ip-protocol**, use **destination udp-port**.
- The same condition cannot specify a destination UDP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.
- Use this condition in combination with the IPv6 condition (**policy condition ipv6**) to configure IPv6 policies for Layer 4 information, services, and service groups.

Examples

```
-> policy condition cond4 destination udp-port 137-138
-> policy condition cond5 ipv6 destination udp-port 140
-> policy condition cond4 no destination udp-port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationTcpPort
   alaQoSConditionDestinationTcpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationTcpPort
   alaQoSAppliedConditionDestinationTcpPortEnd
```

policy condition ethertype

Configures an ethertype value to use for traffic classification.

policy condition *condition_name* **ethertype** *etype*

policy condition *condition_name* **no ethertype**

Syntax Definitions

condition_name	The name of the condition.
etype	The ethertype value, in the range 1536–65535 or 0x600–0xffff hex.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an ethertype value from a condition; however, at least one classification parameter must be associated with a condition.
- Enter a numeric or equivalent hex value for the *etype*.
- On the OmniSwitch 6465, an ethertype value is not supported in policy conditions for IPv6 packets.

Examples

```
-> policy condition cond12 ethertype 8137
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionEthertype
   alaQoSConditionEthertypeStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionEthertype
   alaQoSAppliedConditionEthertypeStatus
```

policy condition established

Configures an established TCP connection as a policy condition. A connection is considered established if the **ack** or **rst** flags in the TCP header of the packet are set.

policy condition *condition_name* **established**

policy condition *condition_name* **no established**

Syntax Definitions

condition_name	The name of the condition.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove **established** from a condition; however, at least one classification parameter must be associated with a condition.
- When an initial TCP connection packet is received only the **syn** flag is set. As a result, TCP packets are only examined if they are not the starting packet.
- Typically this condition is used in combination with **source ip, destination ip**, **source port**, **destination port**, **source tcp-port**, or **destination tcp-port** conditions.
- Note that even though **established** can be used with most action parameters, it is mainly intended for ACL use.

Examples

```
-> policy condition cond2 source ip 192.168.5.10 established
-> policy condition cond3 destination ip 10.255.11.40
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionTcpEstablished
alaQoSAppliedConditionTable
   alaQoSAppliedConditionTcpEstablished
```

policy condition tcpflags

Configures a specific TCP flag value or combination of flag values as a policy condition.

policy condition *condition_name* **tcpflags [any | all] {f | s | r | p | a | u | e | w} mask {f | s | r | p | a | u | e | w}**

policy condition *condition_name* **no tcpflags**

Syntax Definitions

condition_name	The name of the condition.
any	Match on any of the specified TCP flags.
all	Match all specified TCP flags.
f | s | r | p | a | u | e | w	TCP flag value to match (**f**=fin, **s**=syn, **r**=rst, **p**=psh, **a**=ack, **u**=urg, **e**=ecn, and **w**=cwr). *The **e** and **w** flags are currently not supported*.

Defaults

parameter	default
any | **all**	all

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove **tcpflags** from a condition; however, at least one classification parameter must be associated with a condition.
- Use the **any** option to indicate that a match on any one of the specified TCP flags qualifies as a match for the condition. Use the **all** option to indicate that a match on all specified TCP flags is required to qualify as a match for the condition.
- Enter one or more TCP flags after the **any** or **all** keyword to indicate that the value of the flag bit must be set to one to qualify as a match.
- Enter one or more TCP flags after the **mask** keyword to indicate which TCP flags to match.
- If a TCP flag is specified as part of the **mask** but does not have a corresponding match value specified with the **any** or **all** options, then zero is assumed as the match value. For example, **tcpflags all f s mask f s a** looks for the following bit values to determine a match: **f**=1, **s**=1, **a**=0.
- Typically this condition is used in combination with **source ip, destination ip**, **source port**, **destination port**, **source tcp-port**, or **destination tcp-port** conditions.
- Note that even though **tcpflags** can be used with most action parameters, it is mainly intended for ACL use.
- Use **tcpflags** in combination with the IPv6 condition to configure an IPv6 TCP flag policy (for example, **policy condition ipv6 tcpflags**). *Note that IPv6 TCP flag conditions are not supported on the*

OmniSwitch 6560.

Examples

```
-> policy condition tcp-flag tcpflags all f s mask f s a
-> policy condition tcp-flag-ar tcpflags any a r mask a r
-> policy condition tcp-flag-f destination network group Allowed_Resources source
tcp-port 1982 tcpflags any f mask f ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionTcpFlags,
   alaQoSConditionTcpFlagsStatus,
   alaQoSConditionTcpFlagsVal,
   alaQoSConditionTcpFlagsValStatus,
   alaQoSConditionTcpFlagsMask,
   alaQoSConditionTcpFlagsMaskStatus,
alaQoSAppliedConditionTable
   alaQoSAppliedConditionTcpFlags,
   alaQoSAppliedConditionTcpFlagsStatus,
   alaQoSAppliedConditionTcpFlagsVal,
   alaQoSAppliedConditionTcpFlagsValStatus,
   alaQoSAppliedConditionTcpFlagsMask,
   alaQoSAppliedConditionTcpFlagsMaskStatus,
```

policy condition service

Configures a service for a policy condition.

policy condition *condition_name* **service** *service_name*

policy condition *condition_name* **no service**

Syntax Definitions

condition_name	The name of the condition.
service_name	The service name, configured through the **policy service** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a service group from a condition; however, at least one classification parameter must be associated with a condition.
- A policy condition that specifies a service cannot also specify a service group, IP protocol, source IP port, or destination IP port.

Examples

```
-> policy condition cond12 service serv2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service	Configures a service that may be used as part of a policy service group.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
show policy service	Displays information about all particular policy services or a particular policy service configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionService
alaQoSAppliedConditionTable
   alaQoSAppliedConditionService
```

policy condition service group

Associates a policy service group with a policy condition.

policy condition *condition_name* **service group** *service_group*

policy condition *condition_name* **no service group**

Syntax Definitions

condition_name	The name of the condition.
service_group	The service group name. Service groups are configured through the **policy service group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a service group from a condition; however, at least one classification parameter must be associated with a condition.
- A policy condition that specifies a service group cannot also specify a service, IP protocol, source IP port, or destination IP port.

Examples

```
-> policy condition cond12 service group servgroup2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group	Configures a service group and its associated services.
policy condition	Creates a policy condition.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionServiceGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionServiceGroup
```

policy condition icmptype

Configures an ICMP type value to use for traffic classification.

policy condition *condition_name* **icmptype** *type*

policy condition *condition_name* **no icmptype**

Syntax Definitions

condition_name	The name of the condition.
type	The ICMP type value, in the range 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove an ICMP type value from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond12 icmptype 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition icmpcode	Configures an ICMP code value for traffic classification.
policy condition	Creates a policy condition.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionIcmpType
   alaQoSConditionIcmpTypeStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIcmpType
   alaQoSAppliedConditionIcmpTypeStatus
```

policy condition icmpcode

Configures an ICMP code value to use for traffic classification.

policy condition *condition_name* **icmpcode** *code*

policy condition *condition_name* **no icmpcode**

Syntax Definitions

condition_name	The name of the condition.
code	The ICMP code value, in the range 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove an ICMP code value from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond12 icmpcode 150
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition icmptype	Configures an ICMP type value for traffic classification.
policy condition	Creates a policy condition.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionIcmpCode
   alaQoSConditionIcmpCodeStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIcmpCode
   alaQoSAppliedConditionIcmpCodeStatus
```

policy condition ip-protocol

Configures an IP protocol for a policy condition.

policy condition *condition_name* **ip-protocol** *protocol*

policy condition *condition_name* **no ip-protocol**

Syntax Definitions

condition_name	The name of the condition.
protocol	The protocol associated with the flow. The range is 0–255.

Defaults

parameter	default
protocol	6

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a protocol from a condition; however, at least one classification parameter must be associated with a condition.
- If a source or destination port is specified (through the **policy condition source ip-port** or **policy condition destination ip-port** commands), the protocol must be specified.
- The same condition cannot specify an IP protocol with a service or service group.

Examples

```
-> policy condition cond4 ip-protocol 6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition source ip-port	Configures a source IP port number for a policy condition.
policy condition destination ip-port	Configures a destination IP port number for a policy condition.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionIpProtocol
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIpProtocol
```

policy condition ipv6

Configures a policy condition to classify IPv6 traffic.

policy condition *condition_name* **ipv6**

policy condition *condition_name* **no ipv6**

Syntax Definitions

condition_name	The name of the condition.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove IPv6 traffic as a condition; however, at least one classification parameter must be associated with a condition.
- When the **ipv6** keyword is used in a condition, a policy that uses the condition is considered an IPv6 policy. IPv6 policies are effected only on IPv6 traffic. All other IP policies are considered IPv4 policies and are effected only on IPv4 traffic.
- IPv6 Layer 4 policies are supported and are configured using the **ipv6** keyword in a condition that specifies Layer 4 information, services, or service groups. Note that IPv6 Layer 4 policies only work with packets that contain a single header.
- The **icmptype** and **icmpcode** keywords in an IPv6 policy imply the ICMPv6 protocol, not the ICMPv4 protocol.

Examples

```
-> policy condition cond4 ipv6
-> policy condition cond5 ipv6 tos 7
-> policy condition cond6 ipv6 source port 1/1/1
-> policy condition cond7 ipv6 source tcp-port 21
-> policy condition cond8 ipv6 source tcp-port 0-1024
-> policy condition cond6 no ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionIpv6Traffic
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIpv6Traffic
```

policy condition flow-label

Configures an IPv6 flow label value as a policy condition. This value is compared to the flow label value in the IPv6 header.

policy condition *condition_name* **flow-label** *flow_label_value*

policy condition *condition_name* **no flow-label**

Syntax Definitions

condition_name	The name of the condition.
flow_label_value	The flow-label value (0–1048575).

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove the flow label value as a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 flow-label 1500
-> policy condition cond4 no flow-label
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionIpv6FlowLabel
   alaQoSConditionIpv6FlowLabelStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIpv6FlowLabel
   alaQoSAppliedConditionIpv6FlowLabelStatus
```

policy condition tos

Configures the precedence bits in the Type of Service (ToS) byte value for a policy condition.

policy condition *condition_name* **tos** *tos_value* **[mask** *tos_mask***]**

policy condition *condition_name* **no tos**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
tos_value	The Type of Service bits value included in the IP header. The three most significant bits of the byte determine the precedence (i.e, priority) of the frame (0 is the lowest, 7 is the highest).
tos_mask	The mask for the ToS bits, in the range 0–7.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a ToS value from a condition; however, at least one classification parameter must be associated with a condition.
- If a ToS value is specified, a DSCP value may not be specified.

Examples

```
-> policy condition cond2 tos 7
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionTos
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionTos
```

policy condition dscp

Configures the Differentiated Services Code Point (DSCP) for a policy condition. The DSCP value defines the six most significant bits of the DS byte in the IP header.

policy condition *condition_name* **dscp {***dscp_value***[-***value***]} [mask** *dscp_mask***]**

policy condition *condition_name* **no dscp**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
dscp_value[-*value*]	The DiffServ Code Point value, in the range 0–63. Use a hyphen to specify a range of DSCP values for the condition (for example, 10-20).
dscp_mask	The mask for the DiffServ Code Point, in the range 0–63. *Specifying a DSCP mask for a policy condition is not supported on an OmniSwitch 6465.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a DSCP value from a condition; however, at least one classification parameter must be associated with a condition.
- If a DSCP value is specified, a ToS value may not be specified.
- When a DSCP policy condition is configured on one of these switches, QoS automatically calculates the appropriate mask value.

Examples

```
-> policy condition cond4 dscp 10
-> policy condition cond5 dscp 20-30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDscp
   alaQoSConditionDscpMask
   alaQoSConditionDscpEnd
   alaQoSConditionDscpStatus
alaQosAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDscp
   alaQoSAppliedConditionDscpMask
   alaQoSAppliedConditionDscpEnd
   alaQoSAppliedConditionDscpStatus
```

policy condition source mac

Configures a source MAC address for a policy condition.

policy condition *condition_name* **source mac** *mac_address* **[mask** *mac_mask***]**

policy condition *condition_name* **no source mac**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
mac_address	The source MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23)
mac_mask	Optional. The mask for the source MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a source MAC address from a condition; however, at least one classification parameter must be associated with a condition.
- A source MAC address and a source MAC group cannot be specified in the same condition.
- On the OmniSwitch 6465, a source MAC address is not supported in policy conditions for IPv6 packets.

Examples

```
-> policy condition cond2 source mac 00:20:da:05:f6:23
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceMacAddr
   alaQoSConditionSourceMacMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceMacAddr
   alaQoSAppliedConditionSourceMacMask
```

policy condition destination mac

Configures a destination MAC address for a policy condition.

Note. Specifying a destination MAC address and mask of all zeros (00:00:00:00:00:00) as a policy condition can result in the switch dropping all traffic. Only use this type of condition in combination with other policies that will allow desired traffic and/or if a source or destination slot/port is also part of the destination MAC condition.

policy condition *condition_name* **destination mac** *mac_address* **[mask** *mac_mask***]**

policy condition *condition_name* **no destination mac**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
mac_address	The destination MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23).
mac_mask	Optional. The mask for the destination MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a destination MAC address from a condition; however, at least one classification parameter must be associated with a condition.
- A destination MAC address and a destination MAC group cannot be specified in the same condition.
- On the OmniSwitch 6465, a destination MAC address is not supported in policy conditions for IPv6 packets.

Examples

```
-> policy condition cond3 destination mac 00:20:da:05:f6:23
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSource
   alaQoSConditionDestinationMacAddr
   alaQoSConditionDestinationMacMask
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSource
   alaQoSAppliedConditionDestinationMacAddr
   alaQoSAppliedConditionDestinationMacMask
```

policy condition source mac group

Associates a source MAC group with a policy condition.

policy condition *condition_name* **source mac group** *group_name*

policy condition *condition_name* **no source mac group**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
group_name	The name of the source MAC group, configured through the **policy mac group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a source MAC group from a condition; however, at least one classification parameter must be associated with a condition.
- A source MAC address and a source MAC group cannot be specified in the same condition.
- On the OmniSwitch 6465, a source MAC group is not supported in policy conditions for IPv6 packets.

Examples

```
-> policy condition cond4 source mac group mac_group1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy mac group	Configures a MAC group and its associated MAC addresses.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceMacGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceMacGroup
```

policy condition destination mac group

Associates a destination MAC group with a policy condition.

policy condition *condition_name* **destination mac group** *mac_group*

policy condition *condition_name* **no destination**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
mac_group	The name of the destination MAC group, configured through the **policy mac group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a destination MAC group from a policy condition; however, at least one classification parameter must be associated with a condition.
- A destination MAC address and a destination MAC group cannot be specified in the same condition.
- On the OmniSwitch 6465, a source MAC group is not supported in policy conditions for IPv6 packets.

Examples

```
-> policy condition cond5 destination mac group mac_group1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy mac group	Configures a MAC group and its associated MAC addresses.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationMacGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationMacGroup
```

policy condition source vlan

Configures a source VLAN for a policy condition.

policy condition *condition_name* **source vlan** *vlan_id*

policy condition *condition_name* **no source vlan**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
vlan_id	The source VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove a source VLAN from a policy condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond5 source vlan 3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceVlan
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceVlan
```

policy condition inner source-vlan

Configures an inner source VLAN ID as a policy condition. This condition applies to double-tagged VLAN Stacking traffic and is used to classify such traffic based on the inner VLAN ID tag, also known as the customer VLAN ID.

policy condition *condition_name* **inner source-vlan** *vlan_id*

policy condition *condition_name* **no inner source-vlan**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
vlan_id	The inner source VLAN ID (customer VLAN ID) to match on double-tagged packets.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove an inner source VLAN from a policy condition; however, at least one classification parameter must be associated with a condition.
- Policies that use the inner source VLAN condition are referred to as QoS VLAN Stacking policies. These are separate policies from those configured through the VLAN Stacking Service application.

Examples

```
-> policy condition cond5 inner source-vlan 3
-> policy condition cond5 no inner source-vlan
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionInnerSourceVlan
   alaQoSConditionInnerSourceVlanStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionInnerSourceVlan
   alaQoSAppliedConditionInnerSourceVlanStatus
```

policy condition destination vlan

Configures a destination VLAN (multicast only) for a policy condition. Use the **no** form of the command to remove a destination VLAN from a condition.

policy condition *condition_name* **destination vlan** *vlan_id*

policy condition *condition_name* **no destination vlan**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
vlan_id	The destination VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a destination VLAN from a condition; however, at least one classification parameter must be associated with a condition.
- Note that this condition is supported for multicast only policies.

Examples

```
-> policy condition cond4 destination vlan 3 multicast ip any
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationVlan
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationVlan
```

policy condition 802.1p

Configures the 802.1p value for a policy condition.

policy condition *condition_name* **802.1p** *802.1p_value*

policy condition *condition_name* **no 802.1p**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
802.1p_value	The 802.1p value in the 802.1Q VLAN tag for the flow. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove an 802.1p value for a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond3 802.1p 7
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSCondition8021p
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedCondition8021p
```

policy condition inner 802.1p

Configures an inner (customer) source 802.1p value for a policy condition. This condition applies to double-tagged VLAN Stacking traffic and is used to classify such traffic based on the inner 802.1p bit value.

policy condition *condition_name* **inner 802.1p** *802.1p_value*

policy condition *condition_name* **no inner 802.1p**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
802.1p_value	The inner 802.1p value of the inner 802.1Q VLAN tag (customer VLAN) to match on double-tagged packets. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove an 802.1p value for a condition; however, at least one classification parameter must be associated with a condition.
- Policies that use the inner 802.1p condition are referred to as QoS VLAN Stacking policies. These are separate policies from those configured through the VLAN Stacking Service application.

Examples

```
-> policy condition cond3 inner 802.1p 7
-> policy condition cond3 no inner 802.1p
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionInner8021p
   alaQoSConditionInner8021pStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionInner8021p
   alaQoSAppliedConditionInner8021pStatus
```

policy condition source port

Configures a source port number for a policy condition. Use the **no** form of the command to remove a source port number from a condition.

policy condition *condition_name* **source {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

policy condition *condition_name* **no source {port | linkagg}**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number on which the frame is received. Use a hyphen to specify a range of ports (1/5-10). *Specifying a range of ports for a policy condition is not supported on an OmniSwitch 6465.*
*agg_id***[**-*agg_id2***]**	The link aggregate ID on which the frame is received. Use a hyphen to specify a range of IDs (10-15). *A link aggregate policy condition is not supported on the OmniSwitch 6560, OmniSwitch 6900-V72, 6900-C32, and OmniSwitch 9900.*

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove a source port from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond2 source port 3/1/1
-> policy condition cond3 source port 3/2/1-4
-> policy condition cond3 no source port
-> policy condition cond3 source linkagg 10
-> policy condition cond3 source linkagg 15-20
-> policy condition cond3 no source linkagg
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **linkagg** parameter added.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceSlot
   alaQoSConditionSourcePort
   alaQoSConditionSourcePortEnd
   alaQoSConditionSourceChassis
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceSlot
   alaQoSAppliedConditionSourcePort
   alaQoSAppliedConditionSourcePortEnd
   alaQoSAppliedConditionSourceChassis
```

policy condition destination port

Configures a destination port number for a policy condition.

policy condition *condition_name* **destination {port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

policy condition *condition_name* **no destination {port | linkagg}**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number for which the frame is destined. Use a hyphen to specify a range of ports (1/5-10).
*agg_id***[**-*agg_id2***]**	The link aggregate ID for which the frame is destined. Use a hyphen to specify a range of IDs (10-15). *A link aggregate policy condition is not supported on the OmniSwitch 6560, OmniSwitch 6900-V72, 6900-C32, and OmniSwitch 9900.*

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a destination port from a condition; however, at least one classification parameter must be associated with a condition.
- The destination port condition does not apply to routed traffic. Only bridged unicast traffic is supported (bridged multicast and broadcast traffic is not supported).

Examples

```
-> policy condition cond3 destination port 4/2/1
-> policy condition cond4 destination port 4/3/1-4
-> policy condition cond4 no destination port
-> policy condition cond4 destination linkagg 10
-> policy condition cond4 destination linkagg 15-20
-> policy condition cond4 no destination linkagg
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **linkagg** parameter added.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationSlot
   alaQoSConditionDestinationPort
   alaQoSConditionDestinationPortEnd
   alaQoSConditionDestinationChassis
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationSlot
   alaQoSAppliedConditionDestinationPort
   alaQoSAppliedConditionDestinationPortEnd
   alaQoSAppliedConditionDestinationChassis
```

policy condition source port group

Associates a source port group with a policy condition. Use the **no** form of the command to remove a source port group from a condition.

policy condition *condition_name* **source port group** *group_name*

policy condition *condition_name* **no source port group**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
group_name	The name of the source port group. Port groups are configured through the **policy port group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove a source port group from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond6 source port group portgr4
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy port group	Configures a port group and its associated slot and port numbers.
qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourcePortGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourcePortGroup
```

policy condition destination port group

Associates a destination port group with a policy condition. Use the **no** form of the command to remove a destination port group from a condition.

policy condition *condition_name* **destination port group** *group_name*

policy condition *condition_name* **no destination port**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
group_name	The name of the destination port group. Port groups are configured through the **policy port group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove a destination port group from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond6 destination port group portgr4
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy port group	Configures a port group and its associated slot and port numbers.
qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionDestinationPortGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationPortGroup
```

policy condition vrf

Associates a Virtual Routing and Forwarding (VRF) instance with a policy condition.

policy condition *condition_name* **vrf {***vrf_name* | **default}**

policy condition *condition_name* **no vrf**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
vrf_name	The name of the VRF instance to which the QoS policy condition applies.
default	Specifies the default VRF instance.

Defaults

By default, QoS policy conditions are not associated with any VRF instance. The policy applies across all instances.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a VRF instance from a condition; however, at least one classification parameter must be associated with a condition.
- VRF policies are configured in the default VRF, similar to how all other QoS policies are configured. If the VRF name specified does not exist, the policy is not allocated any system resources.
- Policies that do not specify a VRF name are considered global policies and are applied across all VRF instances and VLANs.
- Policies that specify the default VRF apply only to traffic in the default VRF instance.
- Policies that specify a VRF name apply only to traffic in the VRF instance associated with that name.
- The **switch** network group is supported only in VRF policies that specify the default VRF instance. If this group is specified in a global policy (no VRF specified) then the policy is applied across all VRF instances.

Examples

```
-> policy condition cond6 vrf engr-vrf
-> policy condition cond7 vrf default
-> policy condition cond6 no vrf
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionVrfName
   alaQoSConditionVrfNameStatus
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionVrfName
   alaQoSAppliedConditionVrfNameStatus
```

policy condition fragments

Associates TCP packet fragments with a policy condition.

policy condition *condition_name* **fragments**

policy condition *condition_name* **no fragments**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of the command to remove TCP packet fragments from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond6 fragments
-> policy condition cond7 no fragments
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionFragments
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionFragments
```

policy condition appfp-group

Associates an Application Fingerprinting (AFP) application signature group with a policy condition.

policy condition *condition_name* **appfp-group** *group_name*

policy condition *condition_name* **no appfp-group**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
group_name	The name of the AFP application group to which the QoS policy condition applies.

Defaults

N/A.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove an AFP group name from a condition; however, at least one classification parameter must be associated with a condition.
- The **appfp-group** policy condition is used in rules associated with QoS policy lists that are applied to AFP ports running in either the QoS or UNP mode.

Examples

```
-> policy condition cond6 appfp-group my-p2p
-> policy condition cond6 no appfp-group
```

Release History

Release 7.3.2; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionAppFpGroup
   alaQoSConditionAppFpGroupStatus
```

policy condition vxlan

Creates a VXLAN Snooping policy condition to determine the parameters the switch uses to classify incoming encapsulated Virtual eXtensible Local Area Network (VXLAN) packets. Condition parameters may be configured when the condition is created; or parameters may be configured for an existing condition. At least one parameter must be configured for a condition.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the **no** form for keywords to remove a parameter from the condition.

policy condition *condition_name* **vxlan vni** *vxlan_id*
[inner source mac *mac_address* **[mask** *mac_mask***]]**
[inner source mac-group *mac_group***]**
[inner source ip *ip_address* **[mask** *netmask***]]**
[inner source ipv6 *ip6_address* **[mask** *netmask***]]**
[inner ip-protocol *protocol***]**
[inner l4-port {src *src_port* | **dest** *dest_port***}]**
[vxlan-port *udp_port***]**

no policy condition *condition_name*

Syntax Definitions

condition_name	The name of the VXLAN condition. Any alphanumeric string.
vxlan_id	A 24-bit numerical value that identifies traffic for a VXLAN segment. The valid range is 1– 2147483647.

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- A policy condition and a policy action are combined to make a policy rule. See the **policy rule** command.
- Use the **qos apply** command to activate configuration changes.
- If multiple keywords are defined for a single condition, the traffic flow must match all of the parameters in the condition before the rule is enforced.
- Use the **no** form of the command to remove a condition from the switch configuration.
- The **vni** (VXLAN Network Identifier) parameter is required to configure a VM Snooping policy condition. The VXLAN header contains the VNI that is associated with the source MAC address of the Ethernet frame that is encapsulated in a VXLAN packet. The VNI represents the VXLAN segment ID to which the packet belongs.

- The **vxlan-port** condition parameter applies only to the outer header of an encapsulated VXLAN packet. All other **inner** condition parameters apply only to the inner header of the Ethernet frame that was encapsulated in a VXLAN packet.
- When a VXLAN Snooping policy condition is used in a policy rule, the rule is then applied only to traffic on ports that have the VM Snooping feature enabled.
- All existing policy actions are supported in combination with VXLAN Snooping policy conditions; there are no specific policy actions required for policy rules containing VXLAN Snooping policy conditions. Policy actions are applied to the outer header of an encapsulated VXLAN packet.
- See the "Configuring VXLAN Snooping" chapter in the *OmniSwitch AOS Release 8 Data Center Switching Guide* for more information about using VXLAN Snooping policy rules.

Examples

```
-> policy condition cond4 vxlan vni 23000
```

The following is an example of using VM Snooping policy conditions in a policy rule that is added to a UNP policy list:

```
-> policy condition c1 vxlan vni 1234 udp-port 4789
-> policy condition c1 vxlan inner source mac 00:11:22:33:44:00
-> policy condition c1 vxlan inner source ip 10.10.10.10
-> policy action a1 disposition dscp 45
-> policy rule r1 condition c1 action a1 no default-list
-> policy list list1 type UNP
-> policy list list1 rule r1
-> qos apply
```

Release History

Release 7.3.4; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Configures a policy action.
policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionVxlanVni
   alaQoSConditionVxlanVniStatus
   alaQoSConditionVxlanPort
   alaQoSConditionVxlanPortStatus
   alaQoSConditionVmSourceMacAddr
   alaQoSConditionVmSourceMacAddrStatus
   alaQoSConditionVmSourceMacMask
   alaQoSConditionVmSourceMacGroup
   alaQoSConditionVmSourceMacGroupStatus
   alaQoSConditionVmSourceIpAddr
   alaQoSConditionVmSourceIpAddrStatus
   alaQoSConditionVmSourceIpMask
   alaQoSConditionVmSourceIpv6IpAddr
   alaQoSConditionVmSourceIpv6IpAddrStatus
   alaQoSConditionVmSourceIpv6IpMask
   alaQoSConditionVmIpProtocol
   alaQoSConditionVmIpProtocolStatus
   alaQosConditionVmL4SourcePort
   alaQosConditionVmL4SourcePortStatus
   alaQosConditionVmL4DestPort
   alaQosConditionVmL4DestPortStatus
   alaQosConditionVxlanStatus
```

policy condition vxlan inner source mac

Configures a source MAC address as a policy condition for a VM Snooping policy rule. This type of condition applies to the source MAC address of the inner Ethernet frame of an encapsulated VXLAN packet.

policy condition *condition_name* **vxlan inner source mac** *mac_address* **[mask** *mac_mask***]**

policy condition *condition_name* **vxlan no source mac**

Syntax Definitions

condition_name	The name of an existing policy condition.
mac_address	The source MAC address of a VM (inner MAC address of an encapsulated VXLAN frame).
mac_mask	Optional. The mask for the source MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove the VM source MAC address from a condition; however, at least one classification parameter must be associated with a condition.
- The **vxlan** policy conditions are used to filter VXLAN packets received on VM Snooping ports.

Examples

```
-> policy condition c1 vxlan inner source mac 00:11:22:33:44:00
-> policy condition c2 vxlan inner source mac 00:20:da:05:f6:23 mask
ff:ff:ff:ff:ff:ff
-> policy condition c2 vxlan no source mac
```

Release History

Release 7.3.4; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition vxlan	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionVmSourceMacAddr
   alaQoSConditionVmSourceMacAddrStatus
   alaQoSConditionVmSourceMacMask
```

policy condition vxlan inner source mac-group

Configures a source MAC address group as a policy condition for a VXLAN Snooping policy rule. This type of condition checks to see if the source MAC address of the inner Ethernet frame of an encapsulated VXLAN packet matches any of the MAC addresses specified in the MAC address group.

policy condition *condition_name* **vxlan inner source mac-group** *group_name*

policy condition *condition_name* **vxlan no source mac-group**

Syntax Definitions

condition_name	The name of an existing policy condition.
group_name	The name of the source MAC group, configured through the **policy mac group** command.

Defaults

N/A.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove the source MAC address group name from a condition; however, at least one classification parameter must be associated with a condition.
- The **vxlan** policy conditions are used to filter packets received on VXLAN Snooping ports.

Examples

```
-> policy condition c1 vxlan inner source mac-group vm-macs
-> policy condition c1 vxlan no source mac-group
```

Release History

Release 7.3.4; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition vxlan	Creates a VXLAN policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionVmSourceMacGroup
   alaQoSConditionVmSourceMacGroupStatus
```

policy condition vxlan inner source ip

Configures a source IPv4 address as a policy condition for a VXLAN Snooping policy rule. This type of condition applies to the source IP address of the inner Ethernet frame of an encapsulated VXLAN packet.

policy condition *condition_name* **vxlan inner source ip** *ip_address* **[mask** *netmask***]**

policy condition *condition_name* **vxlan no source ip**

Syntax Definitions

condition_name	The name of an existing policy condition.
ip_address	A specific source IP address.
netmask	The network mask for the source IP address (for example, 255.0.0.0, 255.255.0.0).

Defaults

parameter	default
netmask	IP address class

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove the source IP address from a condition; however, at least one classification parameter must be associated with a condition.
- The **vxlan** policy conditions are used to filter VXLAN packets received on VXLAN Snooping ports.

Examples

```
-> policy condition c1 vxlan inner source ip 10.1.1.2
-> policy condition c2 vxlan inner source ip 10.1.1.3 mask 255.0.0.0
-> policy condition c1 vxlan no source ip
```

Release History

Release 7.3.4; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition vxlan	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionVmSourceIpAddr
   alaQoSConditionVmSourceIpAddrStatus
   alaQoSConditionVmSourceIpMask
```

policy condition vxlan inner source ipv6

Configures a source IPv6 address as a policy condition for a VXLAN Snooping policy rule. This type of condition applies to the source IP address of the inner Ethernet frame of an encapsulated VXLAN packet.

policy condition *condition_name* **vxlan inner source ipv6** *ipv6_address* **[mask** *netmask***]**

policy condition *condition_name* **vxlan no source ipv6**

Syntax Definitions

condition_name	The name of an existing policy condition.
ipv6_address	A specific source IPv6 address.
netmask	The network mask for the source IPv6 address.

Defaults

parameter	default
netmask	IPv6 address class

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove the source IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- The **vxlan** policy conditions are used to filter VXLAN packets received on VXLAN Snooping ports.

Examples

```
-> policy condition c1 vxlan inner source ipv6 ::1234:531F:BCD2:F34A
-> policy condition c1 vxlan no source ipv6
```

Release History

Release 7.3.4; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition vxlan	Creates a VXLAN Snooping policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionVmSourceIpv6IpAddr
   alaQoSConditionVmSourceIpv6IpAddrStatus
   alaQoSConditionVmSourceIpv6IpMask
```

policy condition vxlan inner ip-protocol

Configures a an IP protocol number as a policy condition for a VXLAN Snooping policy rule. This type of condition applies to the IP protocol of the inner Ethernet frame of an encapsulated VXLAN packet.

policy condition *condition_name* **vxlan inner ip-protocol** *protocol*

policy condition *condition_name* **vxlan no ip-protocol**

Syntax Definitions

condition_name	The name of an existing policy condition.
protocol	The IP protocol number. The range is 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove the IP protocol number from a condition; however, at least one classification parameter must be associated with a condition.
- The **vxlan** policy conditions are used to filter VXLAN packets received on VXLAN Snooping ports.

Examples

```
-> policy condition c1 vxlan inner ip-protocol 6
-> policy condition c1 vxlan no ip-protocol
```

Release History

Release 7.3.4; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition vxlan	Creates a VXLAN Snooping policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionVmIpProtocol
   alaQoSConditionVmIpProtocolStatus
```

policy condition vxlan inner l4-port

Configures a Layer 4 (UDP or TCP) source port and/or destination port as a policy condition for a VXLAN Snooping policy rule. This type of condition applies to the Layer 4 port of the inner Ethernet frame of an encapsulated VXLAN packet.

policy condition *condition_name* **vxlan inner l4-port {src** *src_port* **| dest** *dest_port***}**

policy condition *condition_name* **vxlan no l4-port**

Syntax Definitions

condition_name	The name of an existing policy condition.
src_port	The source port number. The valid range is 0–65535
dest_port	The destination port number. The valid range is 0–65535

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove the Layer 4 port number from a condition; however, at least one classification parameter must be associated with a condition.
- The **vxlan** policy conditions are used to filter packets received on VXLAN Snooping ports.

Examples

```
-> policy condition c1 vxlan inner l4-port dest 9445
-> policy condition c1 vxlan inner l4-port src 4000
-> policy condition c2 vxlan inner l4-port dest 8100 inner l4-port src 3000
-> policy condition c1 vxlan no l4-port
```

Release History

Release 7.3.4; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition vxlan	Creates a VXLAN Snooping policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQosConditionVmL4SourcePort
   alaQosConditionVmL4SourcePortStatus
   alaQosConditionVmL4DestPort
   alaQosConditionVmL4DestPortStatus
```

policy condition vxlan vxlan-port

Configures a UDP destination port number as a policy condition for a VXLAN Snooping policy rule. This number is found in the outer IP header of an encapsulated VXLAN packet.

policy condition *condition_name* **vxlan vxlan-port** *udp_port*

policy condition *condition_name* **vxlan no vxlan-port**

Syntax Definitions

condition_name	The name of an existing policy condition.
udp_port	The UDP destination port number of the VXLAN packet. The valid range is 0–65535

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove the VXLAN port number from a condition; however, at least one classification parameter must be associated with a condition.
- VXLAN packets use the well-known UDP destination port 4789 by default.
- The **vxlan** policy conditions are used to filter packets received on VXLAN Snooping ports.

Examples

```
-> policy condition c1 vxlan vxlan-port 6000
-> policy condition c1 vxlan 7000
-> policy condition c1 vxlan no vxlan-port
```

Release History

Release 7.3.4; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition vxlan	Creates a VXLAN Snooping policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionVxlanPort
   alaQoSConditionVxlanPortStatus
```

policy action

Configures or deletes a QoS action. A QoS action describes how traffic that matches a particular QoS condition should be treated. It may specify a particular set of bandwidth and queue parameters, or it may simply specify whether the flow is allowed or denied on the switch.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the **no** form for keywords to remove the parameter from the action.

Note that some action parameters may not be supported depending on the platform you are using. Also some action parameters may not be supported with some conditions. See the condition in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

policy action *action_name*
[disposition {accept | drop | deny}]
[shared]
[priority *priority_value***]**
[maximum bandwidth *bps***]**
[maximum depth *bytes***]**
[cir *bps* **[cbs** *bytes***] [pir** *bps***] [pbs** *bytes***] [color-only]**
[cpu priority *priority***]**
[tos *tos_value***]**
[802.1p *802.1p_value***]**
[dcsp *dcsp_value***]**
[map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group***]**
[permanent gateway ip *ip_address***]**
[permanent gateway ipv6 *ipv6_address***]**
[port-disable]
[redirect port *chassis/slot/port***]**
[redirect linkagg *link_agg***]**
[no-cache]
[{ingress | egress | ingress egress | no} mirror {*chassis/slot/port* **| session** *session_id***}**

policy no action *action_name*

Syntax Definitions

action_name	A name for the action, any alphanumeric string.

Defaults

By default, no drop algorithm is configured for the action, and any queues created by the action are not shared.

parameter	default
accept | drop | deny	accept

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Any condition parameters that the hardware supports will be used to classify the traffic; any condition parameters that are not supported by the hardware will not be used to classify traffic, and the event will be logged in the QoS log.
- Bandwidth parameters may be specified when the action is created or may be specified as separate commands.
- Use the **qos apply** command to activate configuration changes.
- Use the **no** form of the command to remove a QoS action from the configuration.
- If the **configuration snapshot** command is entered after the **policy action** command is configured, the resulting ASCII file will include the following additional syntax for the **policy action** command:

  from {cli | ldap | blt}

  This syntax indicates how the action was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in action, this setting is not configurable.

Examples

```
-> policy action action1 accept
```

Release History

Release 7.1.1; command was introduced.
Release 8.6R1; **session** keyword added.

Related Commands

policy condition	Configures a condition associated with the action.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionSource
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionSource
```

policy action disposition

Configures a disposition for a policy action.

policy action *action_name* **disposition {accept | drop | deny}**

policy action *action_name* **no disposition**

Syntax Definitions

action_name	The name of the action.
accept	Specifies that the switch should accept the flow.
drop	Specifies that the switch should silently drop the flow.
deny	Specifies that the switch should drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option will provide the same result as **drop**; that is, the flow is silently dropped.

Defaults

parameter	default
accept | drop | deny	accept

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove a disposition from an action.

Examples

```
-> policy action a3 disposition deny
-> policy action a3 no disposition
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
alaQoSActionDispositionalaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionDisposition
```

policy action shared

Enables bandwidth sharing among multiple QoS rules that use the same maximum bandwidth action.

policy action *action_name* **shared**

policy action *action_name* **no shared**

Syntax Definitions

action_name	The name of the action.

Defaults

By default, queues created by an action are *not* shared.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the **shared** policy action is not specified, then each bandwidth rule will implement a separate instance of the specified bandwidth allocation.
- Use the **no** form of the command to disable sharing.

Example

```
-> policy action action5 maximum bandwidth 10m shared
-> policy action action6 maximum bandwidth 10m shared
-> policy action action5 no shared
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action maximum bandwidth	Creates a maximum bandwidth policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionShared
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionShared
```

policy action priority

Configures the priority for queuing a flow to which the QoS action applies.

policy action *action_name* **priority** *priority_value*

policy action *action_name* **no priority**

Syntax Definitions

action_name	The name of the action.
priority_value	The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a priority value from an action.
- This priority value is independent of 802.1Q, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.

Examples

```
-> policy action action1 priority 1
-> policy action action1 no priority
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPriority
   alaQoSActionPriorityStatus
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPriority
   alaQoSAppliedActionPriorityStatus
```

policy action maximum bandwidth

Configures a maximum bandwidth value for a policy action.

policy action *action_name* **maximum bandwidth** *bps***[k | m | g | t]**

policy action *action_name* **no maximum bandwidth**

Syntax Definitions

action_name	The name of the action.
*bps***[k | m | g | t]**	The maximum amount of bandwidth, in bits-per-second, for all traffic that ingresses on the port. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m, 1g, 1t**).

Defaults

parameter	default
k | m | g | t	**k**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a maximum bandwidth value from an action.
- If the maximum bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number **10** is specified, **10K** is the maximum bandwidth value used. However, if **10G** is specified, the maximum bandwidth value applied is **10** gbps.
- Use the **shared** policy action to enabling sharing of bandwidth across policy rules that specify the same maximum bandwidth action.

Examples

```
-> policy action action3 maximum bandwidth 10000
-> policy action action4 maximum bandwidth 10k shared
-> policy action action5 maximum bandwidth 10k shared
-> policy action action4 no maximum bandwidth
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionMaximumBandwidth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionMaximumBandwidth
```

policy action maximum depth

Configures the maximum queue depth or bucket size assigned to this action, in bytes. The queue depth or bucket size determines the amount of buffer allocated to each queue. When the queue depth or bucket size is reached, the switch starts dropping packets.

policy action *action_name* **maximum depth** *bytes* **[K (kilo)| M (mega) | G (giga) | T (tera)]**

policy action *action_name* **no maximum depth**

Syntax Definitions

action_name	The name of the action.
bytes **[K | M | G | T]**	The maximum queue depth in bytes. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m, 1g**). If the value is entered as an integer, the switch uses the default unit of **K(kilo)**.

Defaults

parameter	default
K | M | G | T	**K**
bytes	**0**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a maximum depth value from a policy action.
- If the maximum depth value is specified as an integer, without an abbreviated unit designation, the value is applied in Kbytes by default. For example, if the number **10** is specified, **10K** bytes is the maximum depth value used. However, if **10G** is specified, the maximum depth value applied is **10G** bytes.
- A maximum depth action is used in combination with a maximum bandwidth action.

Examples

```
-> policy action action2 maximum depth 100
-> policy action action2 no maximum depth
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionMaximumDepth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionMaximumDepth
```

policy action cir

Configures a Tri-Color Marking (TCM) policy action. This type of action includes parameters for Committed Information Rate (CIR), Committed Burst Size (CBS), Peak Information Rate (PIR), and Peak Burst Size (PBS). The TCM policier meters and marks packets red, green, or yellow based on the parameter values of this policy action.

policy action *action_name* **cir** *bps* **[cbs** *bytes***] [pir** *bps***] [pbs** *bytes***] [color-only]**

policy action *action_name* **no cir**

policy action *action_name* **no pir**

Syntax Definitions

action_name	The name of the action.
*bps***[k | m | g | t]**	The maximum amount of bandwidth, in bits-per-second, for all traffic that ingresses on the port. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m, 1g, 1t**).
bytes	The desired value for maximum bucket size, in bytes.
color-only	Disables TCM rate limiting based on the metering results. Packets are only marked the specific color that applies to the level of packet conformance.

Defaults

parameter	default
cir pir *bps*	0
cbs pbs *bytes*	10K
k | m | g | t	**k**

By default, this action enables rate limiting based on TCM marking and metering.

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the TCM parameter values.
- If the **color-only** parameter is specified with this command, the TCM action will only mark packet color; packets are not rate limited based on the metering results. In this case, packets are then subject to any rate limiting specifications as defined in the queue management configuration for the switch.
- This implementation of TCM supports two rate limiting modes: Single-Rate (srTCM) and Two-Rate (trTCM). The srTCM mode marks packets based only on the CIR and the two burst sizes: CBS and PBS. The trTCM mode marks packets based on both the CIR and PIR and their associated CBS and PBS values.

- There is no explicit CLI command to configure the mode (srTCM or trTCM) in which the TCM meter operates. Instead, the mode is determined by the CIR and PIR values configured for the policy action. If the PIR value is greater than the CIR value, trTCM is used. If the PIR value is less than the CIR value, srTCM is used.
- Configuring CIR and CBS is similar to configuring a maximum bandwidth. Configuring CIR and PIR is similar to configuring maximum depth.
- The number of packets counted as a result of the counter color mode setting is displayed using the **show active policy rule** command. These statistics are only shown for those rules that are configured with a TCM policy action.

Examples

The following command examples configure srTCM (the default):

```
-> policy action A3 cir 10M
-> policy action A4 cir 10M cbs 4k
-> policy action A5 cir 10M cbs 4k pir 10M
-> policy action A6 cir 10M cbs 4k pir 10M pbs 4k
-> policy action a7 cir 5M cbs 2k color-only
-> policy action A3 no cir
-> policy action A5 no pir
```

The following command examples configure trTCM (note that PIR is greater than CIR):

```
-> policy action A7 cir 10M cbs 4k pir 20M
-> policy action A8 cir 10M cbs 4k pir 20M pbs 40M
-> policy action a9 cir 5M cbs 1M pbs 10M pbs 2M color-only
-> policy action A7 no cir
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionCIR
   alaQoSActionCIRStatus
   alaQoSActionCBS
   alaQoSActionCBSStatus
   alaQoSActionPIR
   alaQoSActionPIRStatus
   alaQoSActionPBS
   alaQoSActionPBSStatus
   alaQoSActionColorOnly
alaQoSAppliedActionTable
   alaQoSAppliedActionCIR
   alaQoSAppliedActionCIRStatus
   alaQoSAppliedActionCBS
   alaQoSAppliedActionCBSStatus
   alaQoSAppliedActionPIR
   alaQoSAppliedActionPIRStatus
   alaQoSAppliedActionPBS
   alaQoSAppliedActionPBSStatus
   alaQoSAppliedColorOnly
```

policy action cpu priority

Configures a CPU priority policy action.

policy action *action_name* **cpu priority** *priority*

policy action *action_name* **no cpu priority**

Syntax Definitions

action_name	The name of the action.
priority	The CPU queue on which packets destined for the CPU are received. The valid range is 0–31.

Defaults

By default, the CPU priority is set to zero.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

Use the **no** form of this command to remove the CPU priority parameter value.

Examples

```
-> policy action A7 cpu priority 15
-> policy action A8 cpu priority 31
-> policy action A7 no cpu priority
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionCPUPriority
   alaQoSActionCPUPriorityStatus
alaQoSAppliedActionTable
   alaQoSAppliedActionCPUPriority
   alaQoSAppliedActionCPUPriorityStatus
```

policy action tos

Configures a Type of Service (ToS) bits value to be applied to packets in outgoing flows to which the specified policy applies.

policy action *action_name* **tos** *tos_value*

policy action *action_name* **no tos**

Syntax Definitions

action_name	The name of the action.
tos_value	The three-bit priority value in the IP header that should be set on outgoing frames in flows that match the specified policy. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a ToS value from a policy action.
- Note that specifying both ToS and DSCP in the same action is *not* allowed.

Examples

```
-> policy action action3 tos 4
-> policy action action3 no tos
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionTos
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionTos
```

policy action 802.1p

Configures a value to be set in the 802.1p bits of the 802.1Q byte of an outgoing frame for traffic that matches a policy with this action.

policy action *action_name* **802.1p** *802.1p_value*

policy action *action_name* **no 802.1p**

Syntax Definitions

action_name	The name of the action.
802.1p_value	The priority value to be set in 802.1Q frames. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove an 802.1p value from a policy action.
- Note that specifying both ToS and DSCP in the same action is not allowed.

Examples

```
-> policy action action4 802.1p 7
-> policy action action4 no 802.1p
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSAction8021p
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedAction8021p
```

policy action dscp

Configures a Differentiated Services Code Point (DSCP) value to be set in an outgoing flow for traffic that matches rules with this action.

policy action *action_name* **dscp** *dscp_value*

policy action *action_name* **no dscp**

Syntax Definitions

action_name	The name of the action.
dscp_value	The DSCP value to be set, in the range 0–63.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a DSCP value from a policy action.
- Note that specifying both ToS and DSCP in the same action is *not* allowed.

Examples

```
-> policy action action2 dscp 61
-> policy action action2 no dscp
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionDscp
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionDscp
```

policy action map

Configures a mapping group for a policy action.

policy action map {802.1p | tos | dscp} to {802.1p | tos | dscp} using *map_group*

policy action no map

Syntax Definitions

action_name	The name of the action.
802.1p	Indicates that an 802.1p value should be mapped.
tos	Indicates that a ToS value should be mapped.
dscp	Indicates that a DSCP value should be mapped.
map_group	The name of the map group, configured through the **policy map group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When remapping is configured with this command and a flow matches a policy with this remapping action, and the 802.1p, ToS, or DSCP setting in the incoming flow is specified by the map group, the value will be remapped in the outgoing flow according to the map group.
- If the 802.1p, ToS, or DSCP setting in the incoming flow is not a value specified in the map group, the switch will do one of two things:

  If the *remap from* and *remap to* types are the same (802.1p to 802.1p, ToS to ToS, or DSCP to DSCP), the values in the outgoing flow will be unchanged. If the *remap from* and *remap to* types are not the same (for example: 802.1p to ToS), the switch will determine the outgoing 802.1p and ToS based on whether or not the port is trusted or untrusted).
- Use the **no** form of the command to delete the map group from the configuration.

Examples

```
-> policy action a1 map 802.1p to 802.1p using mapGroup2
-> policy action a2 map 802.1p to tos using mapGroup3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy map group	Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.
qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.
show policy map group	Displays information about all pending and applied policy map groups or a particular map group.

MIB Objects

```
alaQoSActionTable
   alaQoSActionMapFrom
   alaQoSActionMapTo
   alaQoSActionMapGroup
alaQoSAppliedActionTable
   alaQoSAppliedActionMapFrom
   alaQoSAppliedActionMapToalaQoSAppliedActionMapGroup
```

policy action permanent gateway-ip

Used for Policy Based Routing (PBR). Routed flows to which this action is applied will be directed to the IP address specified in the action regardless of whether or not a route already exists in the switch routing table.

policy action *action_name* **permanent gateway-ip** *ip_address*

policy action *action_name* **no permanent gateway-ip**

Syntax Definitions

action_name	The name of the action.
ip_address	The destination IP address to which packets will be routed.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of the command to remove a gateway IP address from a policy action.
- If the gateway goes down, the traffic to be routed over the gateway will be dropped.

Examples

```
-> policy action pbr2 permanent gateway-ip 10.10.2.1
-> policy action pbr2 no permanent gateway-ip
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPermanentGatewayIpAddr
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPermanentGatewayIpAddr
```

policy action permanent gateway-ipv6

Used for Policy Based Routing (PBR). Routed flows to which this action is applied will be directed to the IPv6 address specified in the action regardless of whether or not a route already exists in the switch routing table.

policy action *action_name* **permanent gateway-ipv6** *ipv6_address*

policy action *action_name* **no permanent gateway-ipv6**

Syntax Definitions

action_name	The name of the action.
ipv6_address	The destination IPv6 address to which packets will be routed.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of the command to remove a gateway IPv6 address from a policy action.
- If the gateway goes down, the traffic to be routed over the gateway will be dropped.

Examples

```
-> policy action pbr2 permanent gateway-ipv6 2607:f0d0:2001:000a:0000:0000:0010
-> policy action pbr2 no permanent gateway-ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPermanentGatewayIpV6Addr
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPermanentGatewayIpV6Addr
```

policy action port-disable

Administratively disables the source port of the traffic to which this action is applied.

policy action *action_name* **port-disable**

policy action *action_name* **no port-disable**

Syntax Definitions

action_name	The name of the action.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove **port-disable** from the policy action.
- An SNMP trap is sent when a port is administratively disabled through a port disable action or a UserPorts shutdown function.
- To enable a port disabled by this action, use the **interfaces** or **interfaces fec** command to administratively enable the port, or physically disconnect and reconnect the port cable.

Examples

```
-> policy action pd01 port-disable
-> policy action pb02 no port-disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.
interfaces	Administratively enables or disables a port.
interfaces wait-to-restore	Administratively clears the violation that disabled the port or link aggregate and restores the port to enabled status.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPortdisable
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPortdisable
```

policy action redirect port

Redirects all traffic (flooded, bridged, routed, and multicast) matching a redirect policy to the specified port instead of the port to which the traffic was destined.

policy action *action_name* **redirect port** *chassis/slot/port*

policy action *action_name* **no redirect port**

Syntax Definitions

action_name	The name of the action.
chassis	The chassis identifier.
slot/port	The slot and port number that will receive the redirected traffic.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove **redirect port** from the policy action.
- When redirecting routed traffic from VLAN A to VLAN B, the redirect port must belong to VLAN B (tagged or default VLAN).
- Routed packets (from VLAN A to VLAN B) are not modified after they are redirected; the source and MAC address remain the same. In addition, if the redirect port is tagged, the redirected packets will have a tag from the ingress VLAN A.
- If a route exists for the redirected flow, then redirected packets are the final post-routing packets.
- If a route does not exist for the redirected flow, the flow is not redirected to the specified port or link aggregate and is “blackholed”. As soon as a route is available, the flow is then redirected as specified in the policy.
- In most cases, a redirected flow will *not* trigger an update to the routing and ARP tables. If necessary, create a static route for the flow or assign the redirect port to the ingress VLAN (VLAN A) to send packets to the redirect port until a route is available.
- When redirecting bridged traffic on VLAN A, the redirect port must belong to VLAN A (tagged or default VLAN).

Examples

```
-> policy action rp01 redirect port 1/12/1
-> policy action rp01 no redirect port
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionRedirectSlot
   alaQoSActionRedirectPort
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionRedirectSlot
   alaQoSAppliedActionRedirectPort
```

policy action redirect linkagg

Redirects all traffic (flooded, bridged, routed, and multicast) matching a redirect policy to the specified link aggregate ID instead of the link aggregate to which the traffic was destined.

policy action *action_name* **redirect linkagg** *agg_id*

policy action *action_name* **no redirect linkagg**

Syntax Definitions

action_name	The name of the action.
agg_id	The link aggregate ID number (0–32) to assign to the specified VLAN. See the "Link Aggregation Commands" chapter in this guide.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove **redirect linkagg** from the policy action.
- When redirecting routed traffic from VLAN A to VLAN B, the redirect link aggregate ID must belong to VLAN B (tagged or default VLAN).
- Routed packets (from VLAN A to VLAN B) are not modified after they are redirected; the source and MAC address remain the same. In addition, if the redirect link aggregate ID is tagged, the redirected packets will have a tag from the ingress VLAN A.
- If a route exists for the redirected flow, then redirected packets are the final post-routing packets.
- If a route does not exist for the redirected flow, the flow is not redirected to the specified link aggregate ID and is "blackholed". As soon as a route is available, the flow is then redirected as specified in the policy.
- In most cases, a redirected flow will *not* trigger an update to the routing and ARP tables. If necessary, create a static route for the flow or assign the redirect port or link aggregate ID to the ingress VLAN (VLAN A) to send packets to the redirect port until a route is available.
- When redirecting bridged traffic on VLAN A, the redirect port or link aggregate ID must belong to VLAN A (tagged or default VLAN).

Examples

```
-> policy action rp01 redirect linkagg 2
-> policy action rp01 no redirect linkagg 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionRedirectAgg
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionRedirectAgg
```

policy action no-cache

Disables logging of rule entries to the hardware cache.

policy action *action_name* **no-cache**

policy action *action_name* **no no-cache**

Syntax Definitions

action_name	The name of the action.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove **no-cache** from the policy action.
- Recommended for use when applied to traffic going to the switch.

Examples

```
-> policy action nc01 no-cache
-> policy action nc01 no no-cache
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionNocache
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionNocache
```

policy action mirror

Mirrors ingress, egress, or both ingress and egress packets that match a mirroring policy to the specified port.

policy action *action_name* **[ingress | egress | ingress egress] mirror {***chassis/slot/port* | **session** *session_id***}**

policy action *action_name* **no mirror** {*chassis/slot/port* | **session** *session_id*}

Syntax Definitions

action_name	The name of the action.
ingress	Mirrors ingress packets.
egress	Mirrors egress packets.
ingress egress	Mirrors ingress and egress packets.
chassis	The chassis identifier.
slot/port	The slot and port number that will receive the mirrored traffic.
session_id	Mirroring session identifier. *This parameter is supported only on the OmniSwitch 9900.*

Defaults

parameter	default
ingress | egress | ingress egress	**ingress**

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of the command to remove **mirror** from the policy action.
- Use this command to configure a mirror-to-port (MTP) and mirror-to-session action used for policy based mirroring.
- Only one policy-based MTP session is supported at any given time either port-based policy mirroring or session-based policy mirroring. As a result, all mirroring policies must specify the same destination port or same port mirroring session ID.
- Policy based mirroring and the port based mirroring feature can run simultaneously on the same switch.

Examples

```
-> policy action a1 mirror 1/7/1 (default ingress)
-> policy action a1 ingress mirror 1/7/1
-> policy action a1 egress mirror 1/7/1
-> policy action a1 ingress egress mirror 1/7/1
```

```
-> policy action a1 no mirror
-> policy action a1 mirror session 1
```

Release History

Release 7.1.1; command was introduced.
Release 8.6R1; **session** keyword introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionMirrorSlot
   alaQosActionMirrorPort
   alaQosActionMirrorMode
   alaQosActionMirrorModeStatus
```

show policy network group

Displays information about pending and applied policy network groups.

show [applied] policy network group [*network_group***]**

Syntax Definitions

applied	Indicates that only network groups that have been applied should be displayed.
network_group	The name of the policy network group for which you want to display information; or a wildcard sequence of characters for displaying information about network groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Information for all policy network groups displays unless *network_group* is specified.

Examples

```
-> show policy network group
Group Name                      : netg1
  State                         = new,
  Entries                       = 198.206.10.1

-> show policy network group
Group Name                      : group1
  Entries                       = 203.185.129.0 mask 255.255.255.0,
                                  203.185.131.192 mask 255.255.255.192,
                                  203.185.132.0 mask 255.255.252.0,
                                  204.226.0.0 mask 255.255.0.0
```

output definitions

Group Name	The name of the port group, configured through the **policy network group** command.
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Entries	The IP addresses associated with the network group.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy network group	Configures policy network groups.

MIB Objects

```
alaQoSNetworkGroupsTable
   alaNetworkGroupsName
   alaNetworkGroupsSource
alaNetworkGroupTable
   alaNetworkGroupIpAddr
   alaQoSNetworkGroupIpMask
```

show policy service

Displays information about pending and applied policy services.

show [applied] policy service [*service_name***]**

Syntax Definitions

applied	Indicates that only network groups that have been applied should be displayed.
service_name	The name of the service for which you want to display information; or a wildcard sequence of characters for displaying information about services with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Information about all policy services is displayed unless *service_name* is specified.

Examples

```
-> show policy service
Service name                    : s1
  State                         = new,
  Destination UDP port          = 1001-2004
```

output definitions

Service Name	The name of the port group, configured through the **policy service** command.
State	This field appears if the service was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
IPProto	The IP protocol associated with the service.
ScrPort	A source port associated with the service.
DstPort	A destination port associated with the service.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service	Configures a service that may be used as part of a policy service group.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceIpProtocol
   alaQoSServiceSourceIpPort
   alaQoSServiceDestinationIpPort
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceIpProtocol
   alaQoSAppliedSourceIpPort
   alaQoSAppliedServiceDestinationIpPort
```

show policy service group

Displays information about pending and applied policy service groups.

show [applied] policy service group [*service_group***]**

Syntax Definitions

applied	Indicates that only network groups that have been applied should be displayed.
service_group	The name of the service group for which you want to display information; or a wildcard sequence of characters for displaying information about service groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Information for all policy service groups displays unless *service_group* is specified.

Examples

```
-> show policy service group
Group Name                       : mgmt
  State                          = new,
  Entries                        = ftp,
                                   http,
                                   https,
                                   snmp,
                                   ssh,
                                   telnet
```

output definitions

Group Name	The name of the port group, configured through the **policy service group** command.
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Entries	The services associated with the group. Services are configured through the **policy service** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group	Configures a service group and its associated services. A service group may be attached to a policy condition.

MIB Objects

```
alaQoSServiceGroupsTable
   alaQoSServiceGroupsName
   alaQoSServiceGroupsSource
alaQoSAppliedServiceGroupsTable
   alaQoSAppliedServiceGroupsName
   alaQoSAppliedServiceGroupsSource
alaQoSServiceGroupTable
   alaQoSServiceGroupServiceName
alaQoSAppliedServiceGroupTable
   alaQoSAppliedServiceGroupServiceName
```

show policy mac group

Displays information about pending and applied MAC groups.

show [applied] policy mac group [*mac_group***]**

Syntax Definitions

applied	Indicates that only network groups that have been applied should be displayed.
mac_group	The name of the MAC group for which you want to display information; or a wildcard sequence of characters for displaying information about MAC groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Information for all policy MAC groups displays unless *mac_group* is specified.

Examples

```
-> show policy mac group
Group Name                      : mg1
  State                         = new,
  Entries                       = 00:02:9A:44:5E:10 mask 00:00:00:FF:FF:FF,
                                  00:11:01:00:00:01 mask 00:00:00:FF:FF:FF
                                  00:02:9A:44:5E:20
```

output definitions

Group Name	The name of the port group, configured through the **policy mac group** command.
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Entries	The MAC addresses associated with the group.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy mac group	Configures policy MAC groups.

MIB Objects

```
alaQoSMACGroupsTable
   alaQoSMACGroupsName
   alaQoSMACGroupsSource
alaQoSAppliedMACGroupsTable
   alaQoSAppliedMACGroupsName
   alaQoSAppliedMACGroupsSource
alaQoSMACGroupTable
   alaQoSMACGroupMacAddr
   alaQoSMACGroupMacMask
alaQoSAppliedMACGroupTable
   alaQoSAppliedMACGroupMacAddr
   alaQoSAppliedMACGroupMacMask
```

show policy port group

Displays information about pending and applied policy port groups.

show [applied] policy port group [*group_name***]**

Syntax Definitions

applied	Indicates that only network groups that have been applied should be displayed.
group_name	The name of the policy port group for which you want to display information; or a wildcard sequence of characters for displaying information about port groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Information for all policy port groups displays unless *group_name* is specified.

Examples

```
-> show policy port group
Group Name                      : pg1
  State                         = new,
  Entries                       = 1/2/1,
                                  1/3/1,
                                  1/4/1,
                                  3/1/11
```

output definitions

Group Name	The name of the port group, configured through the **policy port group** command or built-in port groups automatically set up by the switch (**Slot01**, **Slot02**, **Slot03**, etc.).
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Entries	The slot/port combinations associated with the port group.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy port group	Configures a port group and its associated slot and port numbers.

MIB Objects

```
alaQoSPortGroupsTable
   alaQoSPortGroupsName
   alaQoSPortGroupsSource
alaQoSAppliedPortGroupsTable
   alaQoSAppliedPortGroupsName
   alaQoSAppliedPortGroupsSource
alaPortGroupTable
   alaQoSPortGroupSlot
   alaQoSPortGroupPort
alaAppliedPortGroupTable
   alaQoSAppliedPortGroupSlot
   alaQoSAppliedPortGroupPort
```

show policy map group

Displays information about pending and applied policy map groups.

show [applied] policy map group [*group_name***]**

Syntax Definitions

applied	Indicates that only network groups that have been applied should be displayed.
group_name	The name of the policy map group for which you want to display information; or a wildcard sequence of characters for displaying information about map groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Information for all policy map groups displays unless *group_name* is specified.

Examples

```
-> show policy map group
Group Name                      : m1
  State                         = new,
  Entries                       = 0:0,
                                  1:9,
                                  2:18,
                                  3:27,
                                  4:36,
                                  5:45,
                                  6:54,
                                  7:63
```

output definitions

Group Name	The name of the map group, configured through the **policy map group** command.
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Entries	The slot/port combinations associated with the port group.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy map group	Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.

MIB Objects

```
alaQoSMapGroupsTable
   alaQoSMapGroupsName
   alaQoSMapGroupsSource
alaQoSAppliedMapGroupsTable
   alaQoSAppliedMapGroupsName
   alaQoSAppliedMapGroupsSource
alaQoSMapGroupTable
   alaQoSMapGroupKey
   alaQoSMapGroupKeyEnd
   alaQoSMapGroupValue
alaQoSAppliedMapGroupTable
   alaQoSAppliedMapGroupKey
   alaQoSAppliedMapGroupKeyEnd
   alaQoSAppliedMapGroupValue
```

show policy action

Displays information about pending and applied policy actions configured on the switch.

show [applied] policy action [*action_name***]**

Syntax Definitions

applied	Displays only actions that have been applied to the QoS configuration for the switch.
action_name	The name of the action for which you want to display information; or a wildcard sequence of characters for displaying information about actions with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Information for all policy actions displays unless *action_name* is specified.
- When the optional **applied** parameter is used, pending QoS actions are not displayed.

Examples

```
-> show policy action
Action name                     : a1
  Commited Information Rate     = 10.0M,
  Commited Burst size           = 5.00M,
  Peak Information Rate         = 20.0M,
  Peak Burst size               = 5.00M

Action name                     : a2
  State                         = new,
  Disposition                   = deny

Action name                     : a3
  State                         = new,
  Priority                      = 7,

-> show applied policy action
Action name                     : a1
  Commited Information Rate     = 10.0M,
  Commited Burst size           = 5.00M,
  Peak Information Rate         = 20.0M,
  Peak Burst size               = 5.00M
```

output definitions

Action Name	The name of the action, configured through the **policy action** command.
State	This field appears if the action was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Policy Action Parameters	Displays the configured policy action parameters.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy action	Creates a policy action. A QoS action is a particular set of bandwidth and queue parameters that may be applied to a flow matching particular QoS conditions.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionSource
   alaQoSActionDisposition
   alaQoSActionShared
   alaQoSActionMinimumBandwidth
   alaQoSActionMaximumBandwidth
   alaQosActionMaximumDepth
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionSource
   alaQoSAppliedActionDisposition
   alaQoSAppliedActionShared
   alaQoSAppliedActionMinimumBandwidth
   alaQoSAppliedActionMaximumBandwidth
   alaQoSAppliedActionMaximumDepth
```

show policy condition

Displays information about pending and applied policy conditions.

show [applied] policy condition [*condition_name***]**

Syntax Definitions

applied	Displays only conditions that have been applied to the QoS configuration for the switch.
condition_name	The name of the condition for which you want to display information; or a wildcard sequence of characters for displaying information about actions with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Information for all policy conditions displays unless *condition_name* is specified.
- When the optional **applied** parameter is used, pending QoS conditions are not displayed.

Examples

```
-> show policy condition
Condition name                  : c1
  Source VLAN                   = 1001

Condition name                  : c2
  State                         = new,
  Source IP                     = 10.2.2.1,
  Destination UDP port          = 17

-> show applied policy condition
Condition name                  : c1
  Source VLAN                   = 1001
```

output definitions

Condition Name	The name of the condition, configured through the **policy condition** command.
State	This field appears if the condition was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Policy Condition Parameters	Displays the configured policy condition parameters.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Creates a policy condition. The condition determines what parameters the switch uses to classify incoming flows.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSource
   alaQoSConditionSourceSlot
   alaQoSConditionSourcePort
   alaQoSConditionSourcePortGroup
   alaQoSConditionDestinationSlot
   alaQoSConditionDestinationPort
   alaQoSConditionDestinationPortGroup
   alaQoSConditionSourceInterfaceType
   alaQoSConditionDestinationInterfaceType
   alaQoSConditionSourceMacAddr
   alaQoSConditionSourceMacMask
   alaQoSConditionSourceMacGroup
   alaQoSConditionDestinationMacAddr
   alaQoSConditionDestinationMacMask
   alaQoSConditionDestinationMacGroup
   alaQoSConditionSourceVlan
   alaQoSConditionDestinationVlan
   alaQoSCondition8021p
   alaQoSConditionSourceIpAddr
   alaQoSConditionSourceIpMask
   alaQoSConditionSourceNetworkGroup
   alaQoSConditionDestinationIpAddr
   alaQoSConditionDestinationIpMask
   alaQoSConditionDestinationNetworkGroup
   alaQoSConditionMulticastIpAddr
   alaQoSConditionMulticastIpMask
   alaQoSConditionMulticastNetworkGroup
   alaQoSConditionTos
   alaQoSConditionDscp
   alaQoSConditionTcpFlags
   alaQoSConditionIpProtocol
   alaQoSConditionSourceIpPort
   alaQoSConditionDestinationIpPort
   alaQoSConditionService
   alaQoSConditionServiceGroup
```

show active policy rule

Displays information about pending and applied policy rules that are active (enabled) on the switch.

show active policy rule [*rule_name***]**

Syntax Definitions

rule_name	The name of the rule for which you want to display information; or a wildcard sequence of characters for displaying information about rules with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **show policy rule** command to display inactive as well as active policy rules.
- Information for all rules is displayed unless *rule_name* is specified.
- Applied rules may or may not be active on the switch. Applied rules are inactive if they have been administratively disabled with the **disable** option in the **policy rule** command.

Examples

```
-> show active policy rule
Rule name                       : r1
  Condition name                = c1,
  Action name                   = a1,
  Packets                       = 4166772,
  Bytes                         = 266665728
```

output definitions

Rule name	The name of the policy rule, configured through the **policy rule** command.
Condition name	The name of the condition configured for this rule.
Action name	The name of the action configured for this rule.
Packets	The number of packets that match this rule.
Bytes	The number of bytes that match this rule.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleEnabled
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleActive
   alaQoSRuleReflexive
   alaQosRuleLog
   alaQosRuleTrapEvents
   alaQosRuleSave
   alaQoSRuleCondition
   alaQoSRuleAction
```

show policy rule

Displays information about pending and applied policy rules.

show [applied] policy rule [*rule_name***]**

Syntax Definitions

applied	Indicates that only policy rules that have been applied should be displayed.
rule_name	The name of the rule for which you want to display information; or a wildcard sequence of characters for displaying information about rules with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Information for all rules is displayed unless *rule_name* is specified.
- Use the **show active policy rule** command to display only active rules that are currently being enforced on the switch.

Examples

```
-> show policy rule
Rule name                       : r1
  Condition name                = c1,
  Action name                   = a1

Rule name                       : r2
  State                         = new,
  Condition name                = c2,
  Action name                   = a1

Rule name                       : r3
  State                         = new,
  Condition name                = c2,
  Action name                   = a2

-> show applied policy rule
Rule name                       : r1
  Condition name                = c1,
  Action name                   = a1
```

output definitions

Rule name	The name of the policy rule, configured through the **policy rule** command.
State	This field appears if the rule was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Condition name	The name of the condition configured for this rule.
Action name	The name of the action configured for this rule.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleEnabled
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleActive
   alaQoSRuleReflexive
   alaQosRuleLog
   alaQosRuleTrapEvents
   alaQosRuleSave
   alaQoSRuleCondition
   alaQoSRuleAction
```

show policy validity period

Displays information about policy validity periods.

show policy validity period [*name***]**

Syntax Definitions

name	The name of the validity period.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Information for all validity periods is displayed unless *name* is specified.
- Use the **show policy rule** command to display the validity period that is associated with a policy rule.

Examples

```
-> show policy validity-period
Validity period name             = tuesday
  State                          = new,
  Days                           = tuesday

Validity period name             = february
  Months                         = february

-> show applied policy validity-period
Validity period name             = february
  Months                         = february
```

output definitions

Validity period name	The name of the policy validity period, configured through the **policy validity-period** command.
State	This field appears if the validity period was created or modified but not yet applied to the QoS configuration. When the **qos apply** command is issued, this field no longer displays.
Days	The days of the week the validity period is active, configured through the **policy validity-period** command. If this field does not appear, then the validity period is not restricted to specific days.
Months	The months during which the validity period is active, configured through the **policy validity-period** command. If this field does not appear, then the validity period is not restricted to specific months.

output definitions

Hours	The time of day the validity period begins and ends, configured through the **policy validity-period** command. If this field does not appear, then the validity period is not restricted to a specific time.
Interval	The date and time a validity period interval begins and ends, configured through the **policy validity-period** command. If this field does not appear, then the validity period is not restricted to a specific date and time interval.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy validity-period	Configures a validity period that specifies days, times, and/or months during which an associated policy rule is in effect.

MIB Objects

```
alaQoSValidityPeriodTable
   alaQoSValidityPeriodName
   alaQoSValidityPeriodSource
   alaQoSValidityPeriodDays
   alaQoSValidityPeriodDaysStatus
   alaQoSValidityPeriodMonths
   alaQoSValidityPeriodMonthsStatus
   alaQoSValidityPeriodHour
   alaQoSValidityPeriodHourStatus
   alaQoSValidityPeriodEndHour
   alaQoSValidityPeriodInterval
   alaQoSValidityPeriodIntervalStatus
   alaQoSValidityPeriodEndInterval
alaQoSAppliedValidityPeriodTable
   alaQoSAppliedValidityPeriodName
   alaQoSAppliedValidityPeriodSource
   alaQoSAppliedValidityPeriodDays
   alaQoSAppliedValidityPeriodDaysStatus
   alaQoSAppliedValidityPeriodMonths
   alaQoSAppliedValidityPeriodMonthsStatus
   alaQoSAppliedValidityPeriodHour
   alaQoSAppliedValidityPeriodHourStatus
   alaQoSAppliedValidityPeriodEndHour
   alaQoSAppliedValidityPeriodInterval
   alaQoSAppliedValidityPeriodIntervalStatus
   alaQoSAppliedValidityPeriodEndInterval
```

show active policy list

Displays information about applied policy lists that are active (enabled) on the switch.

show active policy list [*list_name***]**

Syntax Definitions

list_name	The name of the list for which you want to display information; or a wildcard sequence of characters for displaying information about lists with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Information for all active rules is displayed unless a *list_name* is specified.
- Use the **show policy list** command to display inactive as well as active policy lists.
- Applied lists may or may not be active on the switch. Applied lists are inactive if they have been administratively disabled with the **disable** option in the **policy list** command.
- The display may include any of the following characters:

character	definition
+	Indicates that the policy list has been modified or has been created since the last **qos apply**.
-	Indicates the policy list is pending deletion.
#	Indicates that the policy list differs between the pending/ applied lists.

Examples

```
-> show active policy list
 Group Name                       From  Type    Enabled  Entries
 ---------------------------------+-----+-------+--------+-------------------------
 list1                            cli   unp     Yes      r1
                                                         r2

 +list2                           cli   unp     Yes      r3

 egress_list1                     cli   egress  Yes      r1
                                                         r2
                                                         r3
```

output definitions

Group Name	The name of the policy list. Configured through the **policy list** command. A plus sign (+) preceding a policy list name indicates that the list was modified or created since the last **qos apply**.
From	Where the list originated.
Type	The type of rule (**unp**, **egress**, **appfp**). Configured through the **policy list** command. Note that the default policy list is not shown. Use the **show policy rule** command to display rules that are members of the default policy list.
Enabled	Whether or not the rule is enabled. Configured through the **policy list** command.
Entries	The QoS policy rules that are grouped together in this policy list. Configured through the **policy list** command.

Release History

Release 7.2.1; command was introduced.

Related Commands

show policy list	Displays information about pending and applied policy lists.
show policy rule	Displays information about pending and applied policy rules

MIB Objects

```
alaQoSRuleGroupsTable
   alaQoSRuleDefaultList
   alaQoSRuleGroupsName
   alaQosRuleGroupsSource
   alaQosRuleGroupsType
   alaQosRuleGroupsEnabled
   alaQosRuleGroupsStatus
alaQosAppliedRuleGroupsTable
   alaQosAppliedRuleGroupsName
   alaQosAppliedRuleGroupsSource
   alaQosAppliedGroupsType
   alaQosAppliedGroupsEnabled
   alaQosAppliedRuleGroupsStatus
```

show policy list

Displays information about pending and applied policy lists.

show [applied] policy list [*list_name***]**

Syntax Definitions

applied	Displays only those policy lists that have been applied to the switch configuration.
list_name	The name of the list to display information; or a wildcard sequence of characters for displaying information about lists with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Information for all rules is displayed unless a *list_name* is specified.
- Use the **show active policy list** command to display only active policy lists that are currently enforced on the switch.
- The display may include any of the following characters:

character	definition
+	Indicates that the policy list has been modified or has been created since the last **qos apply**.
-	Indicates the policy list is pending deletion.
#	Indicates that the policy list differs between the pending/ applied lists.

Examples

```
-> show policy list
 Group Name                       From  Type    Enabled  Entries
 ---------------------------------+-----+-------+--------+--------------------------
 list1                            cli   unp     Yes      r1
                                                         r2

 +list2                           cli   unp     Yes      r3
```

```
-> show applied policy list
 Group Name                       From  Type    Enabled  Entries
 ---------------------------------+-----+-------+--------+--------------------------
 list1                            cli   unp     Yes      r1
                                                         r2
```

output definitions

Group Name	The name of the policy list. Configured through the **policy list** command. A plus sign (+) preceding a policy list name indicates that the list was modified or created since the last **qos apply**.
From	Where the list originated.
Type	The type of rule (**unp**, **egress**, **appfp**). Configured through the **policy list** command. Note that the default policy list is not shown. Use the **show policy rule** command to display rules that are members of the default policy list.
Enabled	Whether or not the rule is enabled. Configured through the **policy list** command.
Entries	The QoS policy rules that are grouped together in this policy list. Configured through the **policy list** command.

Release History

Release 7.2.1; command was introduced.

Related Commands

show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy rule	Displays information about pending and applied policy rules

MIB Objects

```
alaQoSRuleGroupsTable
   alaQoSRuleDefaultList
   alaQoSRuleGroupsName
   alaQosRuleGroupsSource
   alaQosRuleGroupsType
   alaQosRuleGroupsEnabled
   alaQosRuleGroupsStatus
alaQosAppliedRuleGroupsTable
   alaQosAppliedRuleGroupsName
   alaQosAppliedRuleGroupsSource
   alaQosAppliedGroupsType
   alaQosAppliedGroupsEnabled
   alaQosAppliedRuleGroupsStatus
```

show policy ipv4-summary

Displays all the IPv4 networks that are currently matched by ACLs on the system.

show policy ipv4-summary [rule *rule_name***]**

Syntax Definitions

rule_name	The name of the policy rule.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specifying the rule name displays the detailed summary for the corresponding rule. If no rule name is specified, then the summary for each rule is displayed in a tabular form.
- If there is an explicit default rule that is set to deny, the same is displayed in the output.

Examples

```
-> show policy ipv4-summary
Legends:
P= Protocol
Act= Action (d = deny, a = accept)

Rule          P     Source IP/          Destination IP/     VRF Name  Act    Hit Count
                    Source Group        Destination Group
------------+----+----------------+----------------------+--------+-------+----------
rle-rule3    IP    224.0.0.0/4          224.0.0.0/4          default   a      30129
rle-rule4    UDP   0.0.0.0/0            0.0.0.0/0            default   d      10202020
rle-rule1    IP    192.168.10.0/*       192.168.20.0/24      guest     a      458723011
rle-rule2    IP    192.168.30.0/24      192.168.10.0/24      enterpr*  a      458723011


-> show policy ipv4-summary rule rle-rule2
Rule name                       : rle-rule2,
Protocol                        : IP,
Source IP                       : 192.168.30.0/24,
Destination IP                  : 192.168.10.0/24,
VRF Name                        : enterprise,
Action                          : Accept,
Hit Count                       : 458723011
```

output definitions

Rule	Name of the rule.
P	The associated IP protocol.
Source IP/ Source Group	The IPv4 address of the source or source group.

output definitions

Destination IP/Destination Group	The IPv4 address of the destination or destination group.
VRF Name	The name of the VRF.
Act	The name of the action.
Hit Count	The sum of packet counts from all NIs matching the corresponding rule.

Release History

Release 8.3.1.R02; command introduced.
Release 8.4.1.R02; OmniSwitch 6860 and 6865 support added.

Related Commands

show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy rule	Displays information about pending and applied policy rules

MIB Objects

N/A

show policy ipv6-summary

Displays all the IPv6 networks that are currently matched by ACLs on the system.

show policy ipv6-summary [rule *rule_name***]**

Syntax Definitions

rule_name	The name of the policy rule.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specifying the rule name displays the detailed summary for the corresponding rule. If no rule name is specified, then the summary for each rule is displayed in a tabular form.
- If there is an explicit default rule that is set to deny, the same is displayed in the output.

Examples

```
-> show policy ipv6-summary
Legends:
P= Protocol
Act= Action (d = deny, a = accept)

Rule        P     Source IP/                VRF Name  Act  Hit Count      Destination IP/
              Source Group                                                   Destination Group
----------+--+-----------------------------+---------+----+---------+------------------------
rle-Rule1  IP  2001:abcd:1100:200::/64       default    a   02020     2020:acdc:1010:100::/64
rle-Rule2  IP 2010:3456:8080:4323:6789::/32 default    d  10101010   2005:dead::/16


-> show policy ip6-summary rule rle-Rule2
Rule name                       : rle-Rule2,
Protocol                        : IP,
Source IP                       : 2001:abcd:1100:200::/64,
Destination IP                  : 2020:acdc:1010:100::/64,
VRF Name                        : default,
Hit Count                       : 458723011
```

output definitions

Rule	Name of the rule.
P	The associated IP protocol.
Source IP/ Source Group	The IPv6 address of the source or source group.

output definitions

Destination IP/Destination Group	The IPv6 address of the destination or destination group.
VRF Name	The name of the VRF.
Act	The name of the action.
Hit Count	The sum of packet counts from all NIs matching the corresponding rule.

Release History

Release 8.3.1.R02; command introduced.
Release 8.4.1.R02; OmniSwitch 6860 and OmniSwitch 6865 support added.

Related Commands

show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy rule	Displays information about pending and applied policy rules

MIB Objects

N/A

37 Policy Server Commands

This chapter describes CLI commands used for managing policies downloaded to the switch from an attached LDAP server. Policy rules can be created on an attached server through the PolicyView GUI application. Policy rules can also be created on the switch directly through CLI or SNMP commands. This chapter describes commands related to managing LDAP policies only. See Chapter 35, "QoS Commands," for information about commands for creating and managing policies directly on the switch.

The policy commands are based on RFC 2251 and RFC 3060.

MIB information for policy server commands is as follows:

Filename: ALCATEL-IND1-POLICY-MIB.mib
Module: alcatelIND1PolicyMIB

The policy server commands are summarized here:

policy server load
policy server flush
policy server
show policy server
show policy server long
show policy server statistics
show policy server rules
show policy server events

policy server load

Downloads policies from an LDAP server. These policies are created through the PolicyView management application.

policy server load

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

Policies are downloaded to the switch from the directory server with the highest preference setting; this server must be enabled and operational (able to bind).

Examples

```
-> policy server load
```

Release History

Release 7.1.1; command introduced.

Related Commands

policy server flush	Removes all cached LDAP policy data from the switch.

MIB Objects

```
serverPolicyDecision
```

policy server flush

Removes all cached LDAP policy data from the switch.

policy server flush

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

Use this command to remove LDAP policies. Policies configured through the CLI or SNMP are not removed.

Examples

```
-> policy server flush
```

Release History

Release 7.1.1; command introduced.

Related Commands

policy server load	Downloads policies from a LDAP server. These policies are created through the PolicyView management application.

MIB Objects

```
serverPolicyDecision
```

policy server

Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

policy server *ip_address* **[port** *port_number***] [admin-state {enable | disable}] [preference** *preference***] [user** *user_name* **password** *password***] [searchbase** *search_string***] [ssl | no ssl]**

no policy server *ip_address* **[port** *port_number***]**

Syntax Definitions

ip_address	The IP address of the LDAP-enabled directory server.
port_number	The TCP/IP port number used by the switch to connect to the directory server.
enable	Enables the specified policy server to download rules to the switch.The policy servers are **up** by default.
disable	Prevents the specified policy server from downloading rules to the switch.
preference	Determines which directory server is used for policy downloads when multiple servers are configured. The range is 0–255. The server with the highest value is used as the policy server. If that server becomes unavailable, the server with the next highest preference value is used for policy downloads.
user_name	The user name for accessing the database entries on the directory server. When spaces are used in the user name, quotation marks must be included: (e.g. “Directory Manager”).
password	The password associated with the user name. The password must match the password defined on the directory server.
search_string	The root of the directory required for searching the policy information. Typically, the *search_string* includes **o=***organization* and **c=***country*. For example, **o=company** and **c=country**.
ssl	Enables a Secure Socket Layer between the switch and the policy server.
no ssl	Disables a Secure Socket Layer between the switch and the policy server.

Defaults

parameter	default
admin	**up**
port_number	389 (SSL disabled) 636 (SSL enabled)
preference	0
ssl | no ssl	**no ssl**

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

If you change the port number, another entry is added to the policy server table; the existing port number is not changed. To remove a port number, use the **no** form of this command with the relevant policy server IP address and the port number you want to remove.

Examples

```
-> policy server 222.22.22.2 port 345 user dirmgr password secret88 searchbase
ou=qos,o=company,c=country
```

Release History

Release 7.1.1; command introduced.

Related Commands

show policy server	Displays information about policies downloaded from an LDAP server.

MIB Objects

```
DIRECTORYSERVERTABLE
   directoryServerAddress
   directoryServerPort
   directoryServerAdminStatus
   directoryServerPreference
   directoryServerUserId
   directoryServerAuthenticationType
   directoryServerPassword
   directoryServerSearchbase
   directoryServerEnableSSL
```

show policy server

Displays information about servers from which policies can be downloaded to the switch.

show policy server

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

This command displays basic information about policy servers. Use the **show policy server long** command to display more details about the servers.

Examples

```
-> show policy server

Server   IP Address    port   enabled  status   primary
------+--------------+-----+---------+--------+--------
   1   208.19.33.112  389      Yes      Up        X
   2   208.19.33.66   400      No       Down      -
```

output definitions

Server	The index number corresponding to the LDAP server.
IP Address	The IP address of the LDAP server.
port	The TCP/IP port number used by the switch to connect to the policy server.
enabled	Whether or not the policy server is enabled.
status	The state of the policy server, **Unkn**, **Up** or **Down**.
primary	Indicates whether the server is the primary server; this server can be used for the next download of policies; only one server is a primary server.

Release History

Release 7.1.1; command introduced.

Related Commands

policy server	Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

MIB Objects

```
directoryServerTable
   directoryServerAddress
   directoryServerPort
   directoryServerAdminState
```

show policy server long

Displays more detailed information about an LDAP policy server.

show policy server long

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

This command displays detailed information about policy servers. Use the **show policy server** command to display basic information about policy servers.

Examples

```
-> show policy server long
LDAP server 0
  IP address           : 155.132.44.98,
  TCP port             : 16652,
  Enabled              : Yes,
  Operational status   : Unkn,
  Preference           : 99,
  Authentication       : password,
  SSL                  : Disabled,
  login DN             : cn=Directory Manager,
  searchbase           : ou:4.1, cn=policyRoot, o=company.fr
  Last load time       : 09/13/01 16:38:18
LDAP server 1
  IP address           : 155.132.48.27,,
  TCP port             : 21890,
  Enabled              : Yes,
  Operational status   : Unkn,
  Preference           : 50,
  Authentication       : password,
  SSL                  : Disabled,
  login DN             : cn=Directory Manager,
  searchbase           : o=company.fr
  Last load time       : 00/00/00 00:00:00
```

output definitions

IP address	The IP address of the policy server.
TCP port	The TCP/IP port number used by the switch to connect to the policy server.

output definitions (continued)

Enabled	Displays whether the policy server is enabled through the PolicyView application.
Operational status	The state of the policy server, **Up** or **Down**.
Preference	Determines which directory server is used for policy downloads when multiple servers are configured. The range is 0–255. The server with the highest value is used as the policy server. If that server becomes unavailable, the server with the next highest preference value is used for policy downloads.
Authentication	Displays **password** if a user name and password was specified for the server through the **policy server** command. Displays **anonymous** if a user name and password are not configured.
login DN	The directory user name.
searchbase	The searchbase name, which is the root of the directory that can be searched for policy download information.
Last load time	The date and time that policies were last downloaded. Values of zero indicate that no policies have been downloaded.

Release History

Release 7.1.1; command introduced.

MIB Objects

```
directoryServerTable
   directoryServerAddress
   directoryServerPort
   directoryServerPreference
   directoryServerAuthenticationType
   directoryServerSearchbase
   directoryServerUserId
   directoryServerPassword
   directoryServerCacheChange
   directoryServerLastChange
   directoryServerAdminStatus
   directoryServerOperStatus
```

show policy server statistics

Displays statistics about policy directory servers.

show policy server statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

This command displays statistics about server downloads. For information about server parameters, use the **show policy server** command.

Examples

```
-> show policy server statistics
Server   IP Address     port   accesses  delta   successes delta  errors  delta
------+--------------+-------+---------+-------+----------+-----+-------+------
   1     155.132.44.98  16652      793     793       295     295       0     0
   2     155.132.48.27  21890        0       0         0       0       0     0
```

output definitions

Server	The index number corresponding to the server.
IP Address	The IP address of the LDAP server.
port	The TCP/IP port number used by the switch to connect to the policy server.
accesses	The number of times the server was polled by the switch to download policies.
delta	The change in the number of accesses since the last time the policy server was accessed.
successes	The number of times the server was polled by the switch to download policies and the policies were successfully downloaded.
delta	The change in the number of successful policy downloads since the last time the policy server was accessed.
errors	The number of errors returned by the server.
delta	The change in the number of errors returned by the server since the last time the policy server was accessed.

Release History

Release 7.1.1; command introduced.

Related Commands

policy server	Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

MIB Objects

```
policyStatsTable
   policyStatsAddress
   policyStatsServerPort
   policyStatsAccessCount
   policyStatsSuccessAccessCount
   policyStatsNotFoundCount
```

show policy server rules

Displays the names of policies originating from a directory server, that have been downloaded to the switch.

show policy server rules

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

This command displays information about policies created on directory servers only. Chapter 35, "QoS Commands," for information about configuring and displaying policies directly on the switch.

Examples

```
-> show policy server rules
Num       name           prio        scope       status
---+------------------+-------+-------------+------------
1             QoSRule1    0      Provisioned    Active
2             QoSrule2    0      Provisioned    Active
```

Fields are defined here:

output definitions

Num	An index number corresponding to the policy rule.
name	The name of the policy rule; only rules configured through PolicyView are displayed in this table.
prio	The priority or preference of the rule. Indicates the order in which rules can be checked to match to the incoming traffic. If two or more rules apply to the traffic, the rule with the highest preference is applied. Preference is determined when the rule is created.
scope	The type of rule. **Provisioned** is the only type valid for the current release.
status	The status of the rule: **Active** indicates that the rule is available in the QoS software on the switch and is available to be applied to the traffic; **notInService** means the rule can be pushed to the QoS software in the future but is not available yet (typically because of a variable validity period); **notReady** indicates that the rule can never be pushed to the QoS software because its validity period has expired or because it has been disabled through SNMP.

Release History

Release 7.1.1; command introduced.

Related Commands

policy server load	Downloads policies from a LDAP server. These policies are created through the PolicyView management application.

MIB Objects

```
policyRuleNamesTable
   policyRuleNamesIndex
   policyRuleNamesName
   policyRuleOperStatus
```

show policy server events

Displays any events related to a directory server on which policies are stored.

show policy server events

Syntax Definitions

N/A

Defaults

The display is limited to 50 events.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

The Policy Manager initialization event is always the first event logged.

Examples

```
-> show policy server events
 Event Time                      event description
-----------------+-------------------------------------------
09/13/01 16:38:15 Policy manager log init
09/13/01 16:38:17 LDAP server 155.132.44.98/16652 defined
09/13/01 16:38:17 LDAP server 155.132.44.98/21890 defined
09/13/01 16:38:18 PDP optimization: PVP day-of-week all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 IP address and mask make bad address change on desination IP
address 155.132.44.98:155.132.44.101
```

output definitions

Event Time	The date and time the policy event occurred.
event description	A description of the event.

Release History

Release 7.1.1; command introduced.

Related Commands

policy server	Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

MIB Objects

```
policyEventTable
   policyEventCode
   policyEventDetailString
   policyEventIndex
   policyEventTime
```

38 AAA Commands

This chapter includes descriptions for authentication, authorization, and accounting (AAA) commands. The commands are used for configuring the type of authentication as well as the AAA servers and the local user database on the switch.

- Authenticated Switch Access. Authenticates users into the switch to manage the switch. User information is stored on a RADIUS, TACACS+, LDAP or information may be stored locally in the switch user database.
- Local user database. User information may be configured for Authenticated Switch Access. For functional management access, users may be allowed to access specific command families or domains.

MIB information for the AAA commands is as follows:

Filename: ALCATEL-IND1-AAA-MIB.mib
Module: alcatelIND1AAAMIB

Filename: ALCATEL-IND1-SYSTEM-MIB.mib
Module: alcatelIND1SystemMIB

A summary of the available commands is listed here:

Authentication servers	**aaa radius-server** **aaa radius-server health-check** **aaa radius unp-profile-precedence** **aaa test-radius-server** **aaa tacacs+-server** **aaa tacacs command-authorization** **aaa ldap-server** **show aaa server** **show aaa server statistics** **aaa radius-server clear-statistics**
Federal Information Processing Standards (FIPS)	**system fips admin-state** **show system fips**
Authenticated Switch Access	**aaa authentication** **aaa console admin-only** **aaa authentication default** **aaa accounting session** **aaa accounting command** **show aaa authentication** **show aaa accounting**

Port-based Network Access Control (Access Guardian)	**aaa device-authentication** **aaa accounting** **aaa accounting radius calling-station-id** **aaa 802.1x re-authentication** **aaa interim-interval** **aaa session-timeout** **aaa session console** **aaa inactivity-logout** **aaa radius nas-port-id** **aaa radius nas-identifier** **aaa radius nas-ip-address** **aaa radius mac-format** **aaa profile** **show aaa device-authentication** **show aaa accounting** **show aaa config** **show aaa radius config** **show aaa radius health-check-config** **show aaa profile** **show aaa session console config**
Local User Database and Partitioned Management	**user** **password** **user password-size min** **user password-expiration** **show user** **show aaa priv hexa**
Password Policy	**user password-size min** **user password-expiration** **user password-policy cannot-contain-username** **user password-policy min-uppercase** **user password-policy min-lowercase** **user password-policy min-digit** **user password-policy min-nonalpha** **user password-history** **user password-size min** **user password-min-age** **user password-expiration** **show user** **show user password-policy**
User Lockout Settings	**user lockout-window** **user lockout-threshold** **user lockout-duration** **user lockout unlock** **show user** **show user lockout-setting**

Authenticated Switch Access - Enhanced Mode	**aaa switch-access mode** **aaa switch-access ip-lockout-threshold** **aaa switch-access banned-ip release** **aaa switch-access priv-mask** **aaa switch-access management-stations admin-state** **aaa switch-access management-stations** **show aaa switch-access mode** **show aaa switch-access ip-lockout-threshold** **show aaa switch-access banned-ip** **show aaa switch-access priv-mask** **show aaa switch-access management-stations** **show aaa switch-access hardware-self-test** **show aaa switch-access process-self-test**
Common Criteria	**aaa common-criteria admin-state** **show aaa common-criteria config** **aaa certificate update-ca-certificate** **aaa certificate update-crl** **aaa certificate generate-rsa-key key-file** **aaa certificate generate-self-signed** **aaa certificate view** **aaa certificate verify ca-certificate** **aaa certificate delete** **aaa certificate generate-csr**
Public Key Infrastructure (PKI)	**ssl pki client validate-certificate admin-state** **ssl pki client mutual-authentication admin-state** **ssl pki server mutual-authentication admin-state** **ssl pki tls version** **show ssl pki config**
Cipher Security Level	**ssl cipher** **show ssl ciphers all** **show ssl ciphers config**
Kerberos Snooping	**kerberos inactivity-timer** **kerberos ip-address** **kerberos server-timeout** **kerberos authentication-pass policy-list-name** **kerberos authentication-pass domain** **clear kerberos statistics** **show kerberos configuration** **show kerberos users** **show kerberos statistics**
Joint Interoperability Test Command (JITC)	**aaa jitc admin-state** **show aaa jitc config**

aaa radius-server

Configures a RADIUS server for Authenticated Switch Access and device authentication.

aaa radius-server *server_name* **host {***hostname* **|** *ip_address* | *ipv6_address***} [***hostname2* **|** *ip_address2* | *ipv6_address2***] {key** *secret* **| hash-key** *hash_secret* **| prompt-key}[salt** *salt* **| hash-salt** *hash_salt***] [retransmit** *retries***] [timeout** *seconds***] [auth-port** *auth_port***] [acct-port** *acct_port***] [vrf-name** *name***] [ssl | no ssl]**

no aaa radius-server *server_name*

Syntax Definitions

server_name	The name of the RADIUS server.
hostname	The host name (DNS name) of the primary RADIUS server. The host name or IP address is required when creating a server.
ip_address | *ipv6_address*	The IPv4 or IPv6 address of the primary RADIUS server. An IP address or host name is required when creating a server.
hostname2	The host name (DNS name) of an optional backup RADIUS server.
ip_address2 | *ipv6_address2*	The IPv4 or IPv6 address of an optional backup RADIUS server.
secret	The shared secret known to the switch and the server, but which is not sent over the network. Can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case-sensitive. Required when creating a server.
hash_secret	A shared secret that the switch saves with a hashing algorithm.
prompt-key	This option enters the secret key in a obscured format rather than as clear text. When this option is selected, press the Enter key. A prompt appears asking for the secret key. Re-enter the key and only if both entries match, the command is accepted. The key provided in this mode is not displayed on the CLI as text.
salt	The input given through ‘salt’ will be used to add randomness to the encryption of the key. The maximum length of the salt is 15 characters and must be in clear text format. By default, system time will be taken as default salt value.
hash-salt	The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt should not exceed 64 characters.
retries	The number of retries the switch makes to authenticate a user before trying the backup server (*hostname2* or *ip_address2*).
seconds	The timeout for server replies to authentication requests.
auth_port	The UDP destination port for authentication requests.
acct_port	The UDP destination port for accounting requests.
name	The name of the VRF to be used to access the server.
ssl	Enables Transport Layer Security (TLS) between the switch and the RADIUS server.
no ssl	Disables Transport Layer Security (TLS) between the switch and the RADIUS server.

Defaults

parameter	default
retries	3
seconds	2
auth_port	1812
acct_port	1813
ssl | no ssl	**no ssl**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- A host name (or IP address) and a secret are required when configuring a server.
- The server and the backup server must both be RADIUS servers.
- Use the **no** form of the command to remove a RADIUS server from the configuration. Only one server can be deleted at a time.
- A host name (or IP address) and a secret key are required when configuring a server.
- If **key** and **hash-key** parameters are both configured, the **hash-key** value is given priority over **key**.
- The user configured or default salt along with the server name will be combined with 'key' and encrypted as a whole, the output of which will be displayed under ‘hash-key'.
- If **salt** and **hash-salt** parameters are both configured, the **hash-salt** value is given priority over **salt**.
- The special character '!' and pure integers will not be accepted as a valid input for both **salt** and **hashsalt**.
- If you want to provide special characters in salt value, give it in between "" double quotes.
- The input given through **salt** and **hash-salt** is encrypted and will be displayed as “hash-salt” in **show configuration snapshot** command.
- Backward compatibility for **salt** and **hash-salt** is not supported. In case of an accidental downgrade, a boot.cfg error is generated for that particular configuration, and re-configuration is required.
- RADIUS server can be configured on any VRF instance or the default VRF instance. However, all the RADIUS servers must reside on the same VRF instance.
- Enabling the RADIUS server health check feature is recommended for each RADIUS server to help improve the user authentication time. Use the **aaa radius-server health-check** command to enable this feature and the **show aaa server** command to determine the reachability status of each RADIUS server on which health check is enabled.

Examples

```
-> aaa radius-server pubs2 host 10.10.2.1 key wwwtoe timeout 5
-> no aaa radius-server pubs2
```

```
-> aaa radius-server radsrv1 host rad1_ipaddr key rad1_secret vrf-name rad_vrf
-> aaa radius-server “Rad1” host 10.10.10.2 key myorg salt mysalt
-> aaa radius-server “Rad1” host 10.10.2.1 key myorg hash-salt
c7f5eee2c0f9b33e72e3482673fb6059

-> aaa radius-server rad1 prompt-key host 10.10.2.1
Enter Key: *******
Confirm Key: *******
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **prompt-key** parameter added.
Release 8.4.1; **IPv6** and **SSL support** for radius server added.
Release 8.6R1; **salt** and **hash-salt** parameters added.

Related Commands

show aaa server	Displays information about AAA servers.
aaa authentication	Specifies the AAA servers to be used for Authenticated Switch Access.
aaa device-authentication	Specifies the AAA servers to use for Access Guardian device authentication.
aaa accounting session	Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

```
aaaServerTable
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasIpv6Address
   aaasHostName2
   aaasIpAddress2
   aaasIpv6Address2
   aaasRadKey
   aaasRetries
   aaasTimout
   aaasRadAuthPort
   aaasRadAcctPort
   aaasVrfName
   aaasRadEnableSsl
   aaasRadSalt
   aaasRadSaltHash
```

aaa radius-server health-check

Enables or disables the RADIUS server health check configuration for the specified RADIUS server. When this feature is enabled, individual RADIUS servers are polled at the specified time interval to determine whether the server is up or down.

aaa radius-server *server_name* **health-check [poling-interval** *seconds* **| username** *user_name* **| password** *password* **| hash-key** *hash_secret* **| failover]**

no aaa radius-server *server_name* **health-check [failover]**

Syntax Definitions

server_name	The name of the RADIUS server for which a health check session is configured.
seconds	The number of seconds after which a health check request is sent to the specified RADIUS server. The valid range is 60–600 seconds.
user_name	The user name (up to 32 characters) to use in polling requests to the server.
password	The password (up to 64 characters) to use in polling requests to the server.
hash_secret	A shared secret that the switch saves with a hashing algorithm.
failover	Triggers an attempt to re-authenticate users assigned to the authentication server down profile when the RADIUS server comes back up before the authentication server down timeout expires.

Defaults

By default, RADIUS server health check is disabled. When health check is enabled without specifying any of the optional parameters, the following default health check parameter values are set for the specified RADIUS server:

parameter	default
seconds	60
user_name	alcatel
password	alcatel
failover	disabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Make sure the specified RADIUS server is defined on the switch before attempting to enable a health check session for that server. See the **aaa radius-server** command for more information on RADIUS server configuration.

- Each RADIUS server with health check enabled is polled at regular intervals (instead of checked sequentially) to determine if the server is up or down. Notification of the server status is then provided to help expedite the authentication process.
- User devices are typically assigned to a UNP authentication server down profile when the authentication server is down (unreachable).
  - If the **failover** option is disabled (the default) for the health check session, re-authentication is not attempted for the profile devices until the authentication server down timeout value expires.
  - If the **failover** option is enabled for the health check session, there is no waiting for the authentication server down timeout value to expire. When the health check session receives notification that a server has transitioned from down to up, a re-authentication attempt is immediately triggered for the profile devices.
- Use the **no** form of this command to disable health check.
- Use the **no** form of this command with the **failover** parameter to disable the failover operation.

Examples

```
-> aaa radius-server rad1 health-check
-> aaa radius-server rad1 health-check polling-interval 300
-> aaa radius-server rad1 health-check username admin password switch failover
-> no aaa radius-server rad1 health-check failover
-> no aaa radius-server rad1 health-check
```

Release History

Release 8.5R4; command introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access and device authentication.
show aaa radius health-check-config	Displays the health check configuration for each RADIUS server.
show aaa server	Displays information about AAA servers configured for the switch.

MIB Objects

```
aaaServerTable
   aaasHostName
   aaasRadHealthCheck
   aaasRadPollingInterval
   aaasRadFailover
   aaasRadUsername
   aaasRadPassword
```

aaa radius unp-profile-precedence

This command can be used to set the precedence to filter ID or tunnel private group ID attributes for selection of UNP profile in the event of both these attributes being returned from the RADIUS server.

aaa radius unp-profile-precedence {**tunnel-private-group-id** | **filter-id**}

Syntax Definitions

tunnel-private-group-id	The tunnel private group ID attribute.
filter-id	The filter ID RADIUS attribute.

Defaults

By default, filter ID will be given precedence over the tunnel private group ID.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> aaa radius unp-profile-precedence tunnel-private-group-id
-> aaa radius unp-profile-precedence filter-id
```

Release History

Release 8.5R4; command introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access and device authentication.
show aaa radius config	Displays the global AAA attribute values and MAC address format.

MIB Objects

```
alaAaaRadUnpProfilePrecedence
```

aaa test-radius-server

RADIUS test tool allows the user to test the RADIUS server reachability from the OmniSwitch. Use this command to start the authentication or accounting test for the specified user name and password.

aaa test-radius-server *server_name* **type {authentication user** *user_name* **password** *password* **[method {md5 | pap}] | accounting user** *user_name***}**

Syntax Definitions

server_name	RADIUS server name for which test has been configured.
authentication | accounting	Type of test to run.
user_name	User name configured on the server.
password	Password for the given user name.
md5 | pap	Authentication method for the test.

Defaults

By default, MD5 is used as the authentication method.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- RADIUS server must be configured on the switch to test the tool.
- The switch must have the following RADIUS server configuration before starting the test tool: RADIUS server name, acct-port, auth-port, secret key, retransmit count, and timeout. See the **aaa radius-server** command for more information on RADIUS server configuration.
- Supports multiple sessions (console, telnet, SSH) to test multiple RADIUS servers.
- The CLI of the user session (console, telnet, SSH) goes in the blocking state when the test is started. In the blocking state, no other command (CLI) is accepted. The blocking state of the CLI prompt of the switch can be terminated by pressing any key.
- Two IP addresses are configurable for a RADIUS server. When the test starts, the requests are sent to the first address. When all the requests to the first address time out, then the requests are sent to the second address.

Examples

```
-> aaa test-radius-server rad1 type authentication user admin password switch
method MD5
-> aaa test-radius-server rad2 type authentication user admin password switch
method pap
-> aaa test-radius-server rad1 type accounting user admin
```

Release History

Release 8.1.1; command introduced.

Related Commands

aaa authentication	Servers for authenticated switch access.
show aaa server	Displays information about AAA servers configured for the switch.

MIB Objects

N/A

aaa tacacs+-server

Configures or modifies a TACACS+ server for Authenticated Switch Access.

aaa tacacs+-server *server_name* **host {***hostname* **|** *ip_address***} [***hostname2* **|** *ip_address2***] {key** *secret* **| prompt-key}[salt** *salt* **| hash-salt** *hash_salt***] [timeout** *seconds***] [port** *port***] [vrf-name** *name***]**

no aaa tacacs+-server *server*

Syntax Definitions

server_name	The name of the TACACS+ server.
hostname	The host name (DNS name) of the primary TACACS+ server. The host name or IP address is required when creating a server.
ip_address	The IP address of the primary TACACS+ server. An IP address or host name is required when creating a server.
hostname2	The host name (DNS name) of an optional backup TACACS+ server.
ip_address2	The IP address of an optional backup TACACS+ server.
secret	The shared secret known to the switch and the server, but which is not sent over the network. Can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case-sensitive. Required when creating a server.
salt	The input given through ‘salt’ will be used to add randomness to the encryption of the key. The maximum length of the salt is 15 characters, and must be in clear text format. By default, the system time will be taken as default salt value.
hash-salt	The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt should not exceed 64 characters.
prompt-key	This option enters the secret key in a obscured format rather than as clear text. When this option is selected, press the Enter key. A prompt appears asking for the secret key. Re-enter the key and only if both the entries match, the command is accepted. Password provided in this mode is not displayed on the CLI as text.
seconds	The timeout for server replies to authentication requests.
port	The port number for the primary TACACS+ server.
name	The name of the VRF to be used to access the server.

Defaults

parameter	default
seconds	2
port	49

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of the command to remove a TACACS+ server from the configuration. Only one server may be deleted at a time.
- A host name (or IP address) and a secret are required when configuring a server.
- If ‘key’ and ‘hash-key’ parameters are configured at a time, hash-key value is given priority over key.
- The user configured or default salt along with the server name will be combined with 'key' and encrypted as a whole, the output of which will be displayed under ‘hash-key'.
- If ‘salt’ and ‘hash-salt’ parameters are configured at a time, hash-salt value is given priority over salt.
- The special character '!' and pure intergers will not be accepted as a valid input for both salt and hashsalt.
- If you want to provide special characters in salt value, give it in between "" double quotes.
- The input given through ‘salt’ and ‘hash-salt’ is encrypted and will be displayed as ‘hash-salt’ in 'show configuration snapshot' command.
- Backward compatibility for ‘salt’ and ‘hash-salt’ is not supported. In case of an accidental downgrade, boot.cfg error is generated for that particular configuration, and re-configuration is required.
- The server and the backup server must both be TACACS+ servers.
- TACACS+ server can be configured on any VRF instance or the default VRF instance. However, all the TACACS+ servers must reside on the same VRF instance.

Examples

```
-> aaa tacacs+-server tpub host 10.10.2.2 key otna timeout 10
-> no aaa tacacs+-server tpub
-> aaa tacacs+-server T1 host 10.10.10.3 key myorg salt salt@123
-> aaa tacacs+-server tacsrv1 host tac1_ipaddr key tac1_secret vrf-name tac_vrf

-> aaa tacacs+-server tac1 prompt-key host 10.10.2.2
Enter Key:  *******
Confirm Key:   *******
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **vrf-name** parameter added.
Release 8.3.1; **prompt-key** parameter added.
Release 8.6R1; **salt** and **hash-salt** parameters added.

Related Commands

show aaa server	Displays information about AAA servers.
aaa authentication	Specifies the AAA servers to be used for Authenticated Switch Access.
aaa accounting session	Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

```
aaaServerTable
   aaasName
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasTacacsKey
   aaasTimout
   aaasTacacsPort
   aaasVrfName
   aaasRadSalt
   aaasRadSaltHash
```

aaa tacacs command-authorization

Configures a command based authorization in TACACS+ server for authenticated switch.

aaa tacacs command-authorization {enable | disable}

Syntax Definitions

enable	Enable command based authorization in TACACS+ server.
disable	Disable command based authorization. This enables partition-management family based authorization in TACACS+ server.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- This command is applicable only for CLI commands.
- If this command is enabled, then in the TACACS+ server the authorization of every command executed on the switch is command based. CLI commands executed on the switch are sent for authorization to the TACACS+ server along with-mode of operation (read or read-write). After authorization, the server will send the response message to the TACACS+ client.
- If the command is disabled, then in the TACACS+ server the authorization is partition-management family based.
- Use **show configuration snapshot aaa** command to view the configuration details of this command.

Examples

```
-> aaa tacacs command-authorization enable
-> aaa tacacs command-authorization disable
```

Release History

Release 8.3.1; command was introduced.

Related Commands

show aaa server	Displays information about AAA servers.

MIB Objects

```
alaAaaAuthConfig
   alaAaaTacacsServerCmdAuthorization
```

aaa ldap-server

Configures or modifies an LDAP server for Authenticated Switch Access.

aaa ldap-server *server_name* **host {***hostname* | *ip_address***} [***hostname2* | *ip_address2***] dn** *dn_name* **{password** *super_password* | **prompt-password}[salt** *salt* | **hash-salt** *hash_salt***] [base** *search_base***] [retransmit** *retries***] [timeout** *seconds***] [ssl | no ssl] [port** *port***] [vrf-name** *name***]**

no aaa ldap-server *server-name*

Syntax Definitions

server_name	The name of the LDAP server.
hostname	The host name (DNS name) of the primary LDAP server. The host name or IP address is required when creating a server.
ip_address	The IP address of the primary LDAP server.
hostname2	The host name (DNS name) of the backup LDAP server.
ip_address2	The IP address of a backup host for the LDAP server.
dn_name	The super-user or administrative distinguished name in the format recognized by the LDAP-enabled directory servers. For example: **cn=manager**. Must be different from the *search-base* name and must be in a format supported by the server. Required when creating a new server.
super_password	The super-user password recognized by the LDAP-enabled directory servers. The password may be clear text or hexadecimal format. Required when creating a new server.
prompt-password	This option enters the super-user password in a obscured format rather than as clear text. When this option is selected, press the Enter key. A password prompt appears asking for the super-user password. Re-enter the password and only if both the passwords match, the command is accepted. Password provided in this mode is not displayed on the CLI as text.
salt	The input given through ‘salt’ will be used to add randomness to the encryption of the key. The maximum length of the salt is 15 characters and must be in clear text format. By default, the system time will be taken as default salt value.
hash-salt	The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt should not exceed 64 characters.
search_base	The search base recognized by the LDAP-enabled directory servers. For example, **o=company** or **c=country**. Must be different from the *dn_name*. Required when creating a new server.
retries	The number of retries the switch makes to the LDAP server to authenticate a user before trying the backup server.
seconds	The timeout in seconds for server replies to authentication requests from the switch.
ssl	Enables Transport Layer Security (TLS) between the switch and the LDAP server.

no ssl	Disables Transport Layer Security (TLS) between the switch and the LDAP server.
port	The port number for the primary LDAP server and any backup server. Must match the port number configured on the server.
name	The name of the VRF to be used to access the server.

Defaults

parameter	default
port	389 (SSL disabled) 636 (SSL enabled)
retries	3
seconds	2
ssl | no ssl	**no ssl**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The *dn_name* must be different from the *search_base* name.
- Use the **no** form of the command to remove an LDAP server from the configuration. Only one server may be removed at a time.
- The port number configured on the switch must match the port number configured for the server.
- If ‘salt’ and ‘hash-salt’ parameters are configured at a time, hash-salt value is given priority over salt.
- The special character '!' and pure intergers will not be accepted as a valid input for both salt and hashsalt.
- If you want to provide special characters in salt value, give it in between "" double quotes.
- The input given through ‘salt’ and ‘hash-salt’ is encrypted and will be displayed as ‘hash-salt’ in 'show configuration snapshot' command.
- Backward compatibility for ‘salt’ and ‘hash-salt’ is not supported. In case of an accidental downgrade, boot.cfg error is generated for that particular configuration, and re-configuration is required.
- LDAP server can be configured on any VRF instance or the default VRF instance. However, all the LDAP servers must reside on the same VRF instance.

Examples

```
-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager password tpub base c=us
retransmit 4
-> aaa ldap-server omnivista host 1.2.3.4 dn "cn=DirMgr, o=alcatel.com" password
somepass base "ou=People, o=alcatel.com" vrf-name ldap_vrf
-> no aaa ldap-server topanga5

-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager prompt-password base c=us
```

```
retransmit 4
Enter Password:  *******
Confirm Password:   *******

-> aaa ldap-server L1 host 10.10.10.5 dn cn=manager password tpub base c=us salt
mysalt
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **vrf-name** parameter added.
Release 8.3.1; **prompt-password** parameter added.
Release 8.6R1; **salt** and **hash-salt** parameters added.

Related Commands

show aaa server	Displays information about AAA servers.
aaa authentication	Specifies the AAA servers to be used for authenticated switch access.
aaa accounting session	Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

```
aaaServerTable
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasLdapPort
   aaasLdapDn
   aaasLdapPasswd
   aaasLdapSearchBase
   aaasLdapServType
   aaasRetries
   aaasTimeout
   aaasLdapEnableSsl
   aaasVrfName
   aaasLdapSaltHash
   aaasLdapPasswdHash
```

system fips admin-state

Enable or disable the Federal Information Processing Standards (FIPS) mode on the switch.

system fips admin-state {enable | disable}

Syntax Definitions

enable | disable	Enables or disables the FIPS mode.

Defaults

By default, the FIPS mode is disabled on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enabling or disabling FIPS mode takes effect only after a switch reboot. The FIPS mode configuration is persistent across reboots.
- When FIPS mode is disabled, all other existing cryptographic algorithms will be supported.
- A FIPS supported client is required to access the switch in FIPS enabled mode. For example, Absolute Telnet.
- Other unsecured management interfaces, such as Telnet or FTP, have to be manually disabled after FIPS mode is enabled to achieve a completely secure device.

Examples

```
-> system fips admin-state enable
WARNING: FIPS Admin State only becomes Operational after write memory and reload

-> system fips admin-state disable
WARNING: FIPS Admin State only becomes Operational after write memory and reload
```

Release History

Release 8.1.1; command introduced.

Related Commands

show system fips	Show the configured and running status of the FIPS mode on the Switch.

MIB Objects

```
systemFipsAdminState
```

aaa authentication

Configures the interface for Authenticated Switch Access and specifies the server(s) to be used. This type of authentication gives users access to manage the switch.

aaa authentication {console | telnet | ftp | http | snmp | ssh | default} *server1* **[***server2***...] [local]**

no aaa authentication [console | telnet | ftp | http | snmp | ssh | default]

Syntax Definitions

console	Configures Authenticated Switch Access through the console port.
telnet	Configures Authenticated Switch Access for any port used for Telnet.
ftp	Configures Authenticated Switch Access for any port used for FTP.
http	Configures Authenticated Switch Access for any port used for Web-based management.
snmp	Configures Authenticated Switch Access for any port used for SNMP.
ssh	Configures Authenticated Switch Access for any port used for Secure Shell.
default	Configures Authenticated Switch Access for any port using any service (**telnet**, **ftp**, etc.). Note that SNMP access is enabled only if an LDAP or local server is specified with the command.
server1	The name of the authentication server used for Authenticated Switch Access. At least one server is required. The server may be a RADIUS, TACACS+, LDAP, or the local user database. RADIUS, TACACS+, and LDAP server names are set up through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.
server2...	The names of backup servers for Authenticated Switch Access. Up to 3 backups may be specified (including **local**). These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.
local	Specifies that the local user database will be a backup for the authentication servers. If you want to use the local user database as the only authentication server, specify **local** for *server1*.

Defaults

- At switch startup, Authenticated Switch Access is available through console port via the local database. Authentication for other management interfaces (Telnet, FTP, etc.) is disabled.
- The default user on the switch is **admin**, and **switch** is the password.
- Remote authentication is not supported on secondary CMMs or Slave chassis. Use local authentication on secondary CMMs and Slave chassis.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The server type may be RADIUS, TACACS+, LDAP, or the local user database. Up to 4 servers may be configured for an interface type; at least one is required. Each server name should be separated by a space.
- The switch uses ***only the first available server*** in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.
- If the local switch database will be used as the only authentication server, specify **local** for *server1*. If **local** is specified as a backup server, it should be entered last in the list of servers. The local user database is always available if the switch is up.
- Only LDAP or the local database may be used for authenticated SNMP management.
- If Secure Shell (**ssh**) is enabled, Telnet and FTP should be disabled.

Examples

```
-> aaa authentication telnet pubs1
-> no aaa authentication telnet
-> aaa authentication default pubs2 pubs3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for Authenticated Switch Access.
user	Configures user information for the local database on the switch.
show aaa server	Displays information about servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAuthSATable
   aaatsInterface
   aaasName
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
```

aaa console admin-only

Enables or disables the user restriction for all users except the user “admin” from accessing the switch through the secure console session.

aaa console admin-only {enable | disable}

Syntax Definitions

enable	Restricts all users from accessing the switch through the secure console session expect the user “admin”. Only user “admin” can access the switch through the secure console session.
disable	Disables the user restrictions.

Defaults

By default, console admin-only is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enable this feature to restrict all users except user “admin” from accessing the switch through the secure console session.

Examples

```
-> aaa console admin-only enable
-> aaa console admin-only disable
```

Release History

Release 8.3.1 R02; command was introduced.

Related Commands

user	Configures user information for the local database on the switch.

MIB Objects

```
aaaAsaAccessConsoleAdminOnly
```

aaa authentication default

Sets the authenticated switch access type to the default server setting.

aaa authentication {console | telnet | ftp | http | snmp | ssh} default

Syntax Definitions

console	Configures the default Authenticated Switch Access server setting for the console port.
telnet	Configures the default Authenticated Switch Access server setting for Telnet.
ftp	Configures the default Authenticated Switch Access server setting for FTP.
http	Configures the default Authenticated Switch Access server setting for Web-based management.
snmp	Configures the default Authenticated Switch Access server setting for any port used for SNMP.
ssh	Configures the default Authenticated Switch Access server setting for any port used for Secure Shell.

Defaults

By default, the default Authenticated Switch Access server setting does not include any servers.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **aaa authentication** command to set the default servers.

Examples

```
-> aaa authentication telnet default
-> aaa authentication default default
```

Release History

Release 7.1.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access.
aaa tacacs+-server	Configures or modifies an LDAP server for Authenticated Switch Access.
user	Configures user information for the local database on the switch.
show aaa server	Displays information about servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAuthSATable
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
```

aaa accounting session

Configures an accounting server or servers for authenticated switch sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting session *server1* **[***server2***...] [local]**

no accounting session

Syntax Definitions

server1	The name of the RADIUS, TACACS+, or LDAP server used for accounting of authenticated switch sessions. At least one server is required. RADIUS, TACACS+, and LDAP server names are set up through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.
server2...	The names of backup servers. Up to 3 backups may be specified (including **local**); each server name should be separated by a space. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.
local	Local accounting is done through the Switching Logging feature on the switch.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to disable accounting for Authenticated Switch Access.
- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The servers may be RADIUS, TACACS+, LDAP servers, and/or the local Switch Logging facility.
- If **local** is specified as *server1*, the switch will ***only*** use the local Switching Logging facility for accounting.
- If **local** is specified as a backup, it should be entered last in the list of servers. The Switch Logging facility is always available if the switch is up.
- The switch uses ***only the first available server*** in the list for accounting. For example, if *server1* is not available, the switch will use *server2*.
- RADIUS, TACACS+, and LDAP servers may each have an additional backup specified through the **aaa radius-server**, **aaa tacacs+-server**, and **aaa ldap-server** commands.

Examples

```
-> aaa accounting session ldap1 radius2 local
-> no aaa accounting session
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show aaa accounting	Displays information about accounting servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAcctsaTable
   aaacsName1
   aaacsName2
   aaacsName3
   aaacsName4
```

aaa accounting command

Enables or disables the server for command accounting. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting command *server1* **[***server2***...] [local]**

no accounting command

Syntax Definitions

server1	The name of the TACACS+ server used for command accounting. At least one server is required. TACACS+ server names are set up through the **aaa tacacs+-server** commands.
server2...	The names of TACACS+ backup servers. Up to 3 backups may be specified; each server name should be separated by a space. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.
local	Local accounting is done through the Switching Logging feature on the switch.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to disable command accounting.
- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The servers can be only TACACS+ servers.
- The switch uses ***only the first available server*** in the list for accounting. For example, if *server1* is not available, the switch will use *server2*.
- TACACS+ server may each have an additional backup specified through the **aaa tacacs+-server** command.

Examples

```
-> aaa accounting command tacacs1 tacacs2 tacacs3
-> no aaa accounting command
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show aaa accounting	Displays information about accounting servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAcctCmdTable
   aaacmdSrvName1
   aaacmdSrvName2
   aaacmdSrvName3
   aaacmdSrvName4
```

aaa device-authentication

Configures the switch to use RADIUS servers for 802.1X, MAC, and Captive Portal device authentication.

aaa device-authentication {802.1x | mac | captive-portal} *server1* **[***server2***] [***server3***] [***server4***]**

no device-authentication {802.1x | mac | captive-portal}

Syntax Definitions

802.1x	Use the specified RADIUS server to authenticate 802.1X users.
mac	Use the specified RADIUS server for MAC authentication.
captive-portal	Use the specified RADIUS server for Captive Portal authentication.
server1	The name of the RADIUS authentication server to use for the specified type of authentication. (*Note that only RADIUS servers are supported for these types of authentication.*) At least one server is required. RADIUS server names are configured through the **aaa radius-server** command.
server2...server4	The names of backup servers used for authentication. Up to 3 backups may be specified; include a space between each server name. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a RADIUS server assignment for a specific authentication type.
- Up to 4 RADIUS servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The switch uses ***only the first available server*** in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS servers may each have an additional backup specified through the **aaa radius-server** command.
- Configuring the RADIUS servers to use for 802.1X, MAC, and Captive Portal authentication is required to support authentication and classification of devices connected to Universal Network Profile (UNP) ports.

Examples

```
-> aaa device-authentication 802.1x rad1
-> aaa device-authentication 802.1x rad1 rad2
-> no aaa device-authentication 802.1x

-> aaa device-authentication mac rad1
-> aaa device-authentication mac rad1 rad2
-> no aaa device authentication mac

-> aaa device-authentication captive-portal rad1
-> aaa device-authentication captive-portal rad1 rad2
-> no aaa device-authentication captive-portal
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.4; **802.1x** parameter added.
Release 8.1.1; **captive-portal** parameter added.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for authenticated switch access or device authentication.
unp port-type	Enables or disables UNP port-based access control on a port.
show aaa device-authentication	Displays a list of RADIUS servers assigned to provide 802.1X or MAC authentication.

MIB Objects

```
AaaAuthDATable
   aaaDaName1
   aaaDaName2
   aaaDaName3
   aaaDaName4
```

aaa accounting

Configures RADIUS server accounting or local Switch Logging (syslog) accounting for 802.1X, MAC, and Captive Portal authenticated device sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting {802.1x | mac | captive-portal} {*server1* **[***server2***...] | syslog** *ip_address* **[port** *udp_port***]}**

no accounting {802.1x | mac | captive-portal}

Syntax Definitions

802.1x	Enables the specified RADIUS or syslog server to log accounting of 802.1X authenticated sessions.
mac	Enables the specified RADIUS or syslog server to log accounting for MAC authenticated sessions.
captive-portal	Enables the specified RADIUS or syslog server to log accounting for Captive Portal authenticated sessions.
server1	The name of the RADIUS server used for accounting of authenticated switch sessions. At least one server is required. RADIUS server names are configured through the **aaa radius-server** command.
server2...	The names of backup servers. Up to 3 backups may be specified; each server name should be separated by a space. These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.
ip_address	The IP network address for syslog accounting.
udp_port	The UDP port number for syslog accounting.

Defaults

By default, no RADIUS server or syslog accounting is configured for the switch.

parameter	default
udp_port	514

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to disable accounting for device authentication sessions.
- Up to 4 RADIUS accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The switch uses ***only the first available server*** in the list for accounting. For example, if *server1* is not available, the switch will use *server2*.

- Accounting with the local syslog facility is not allowed if RADIUS accounting is already configured. In other words, configure either RADIUS *or* syslog accounting.
- RADIUS servers may each have an additional backup specified through the **aaa radius-server** command.

Examples

```
-> aaa accounting 802.1x rad1
-> aaa accounting 802.1x rad1 rad2 rad3 rad4
-> aaa accounting 802.1x syslog 10.135.67.99 port 8000
-> no aaa accounting 802.1x

-> aaa accounting mac rad1
-> aaa accounting mac rad1 rad2
-> aaa accounting mac syslog 10.135.67.99 port 8000
-> no aaa accounting mac

-> aaa accounting captive-portal rad1
-> aaa accounting captive-portal rad1 rad2 rad3
-> aaa accounting captive-portal syslog 10.135.67.99 port 8000
-> no aaa accounting captive-portal
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show aaa accounting	Displays the accounting server configuration for the switch.

MIB Objects

```
aaaAcctDATable
   aaacdInterface
   aaacdName1
   aaacdName2
   aaacdName3
   aaacdName4
   aaacdSyslogIPAddrType
   aaacdSyslogIPAddr
   aaacdSyslogUdpPort
```

aaa accounting radius calling-station-id

Configures the RADIUS Calling-Station-Id attribute for the specified accounting session type.

aaa accounting {802.1x | mac | captive-portal} radius calling-station-id {mac-address | ip-address}

Syntax Definitions

802.1x	Configures the attribute for 802.1X accounting sessions.
mac	Configures the attribute for MAC accounting sessions.
captive-portal	Configures the attribute for Captive Portal accounting sessions.
mac-address	Sets the Calling Station ID to the MAC address of the user.
ip-address	Sets the Calling Station ID to the IP address of the user.

Defaults

By default, the RADIUS Calling -Station-Id attribute value is set to the MAC address of the user.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Configuring the Calling-Station-Id attribute is not allowed if the accounting server configuration is set to use local Switch Logging (syslog) for the specified accounting session type (802.1x, MAC, or Captive Portal).
- The Calling Station ID attribute is defined in a RADIUS Accounting-Request message that is sent to the RADIUS accounting server.

Examples

```
-> aaa accounting 802.1x radius calling-station-id ip-address
-> no aaa accounting 802.1x radius calling-station-id ip-address
-> aaa accounting 802.1x radius calling-station-id mac-address

-> aaa accounting mac radius calling-station-id ip-address
-> no aaa accounting mac radius calling-station-id ip-address
-> aaa accounting mac radius calling-station-id mac-address

-> aaa accounting captive-portal radius calling-station-id ip-address
-> no aaa accounting onex radius calling-station-id ip-address
-> aaa accounting captive-portal radius calling-station-id mac-address
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show aaa accounting	Displays the AAA accounting configuration.

MIB Objects

```
aaaAcctDATable
   aaacdInterface
   aaacdCallngStationId
```

aaa 802.1x re-authentication

Configures the automatic re-authentication of authenticated 802.1X users.

aaa 802.1x re-authentication {enable | disable | interval *seconds* **| trust-radius {enable | disable}}**

Syntax Definitions

enable	Enables re-authentication of 802.1X users.
disable	Disables re-authentication of 802.1X users.
seconds	The amount of time the switch waits before triggering re-authentication of 802.1X users. The valid range is 600–7200 seconds.
trust-radius enable	Directs the switch to use the Session-Timeout attribute value for the re-authentication time interval. This attribute is returned from the RADIUS server in an Accept-Accept message.
trust-radius disable	Directs the switch to use the locally configured re-authentication time interval value.

Defaults

By default, 802.1X re-authentication is disabled for the switch. When re-authentication is enabled, the following default values apply:

parameter	default
seconds	3600
trust-radius enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The re-authentication time interval is triggered when 802.1X re-authentication is enabled.
- When the re-authentication time interval is changed, the new value does not apply to existing authenticated 802.1X users until the user is flushed out or when the user is authenticated again. Any new 802.1X users are re-authenticated based on the current time interval setting.
- When the trust RADIUS option is enabled, the Session-Timeout attribute value received from the RADIUS server overrides the locally configured value for the switch.
- AAA profile settings for 802.1x re-authentication take precedence over global 802.1x re-authentication settings configured with this command. For example, if the global trust RADIUS option is enabled and the AAA profile trust RADIUS option is disabled (the default), the trust RADIUS status is disabled on the UNP port when the AAA profile is assigned to that port.

Examples

```
-> aaa 802.1x re-authentication enable
-> aaa 802.1x re-authentication enable interval 7200
-> aaa 802.1x re-authentication enable trust-radius enable
-> aaa 802.1x re-authentication enable interval 7200 trust-radius enable
-> aaa 802.1x re-authentication interval 7200 trust-radius disable
-> aaa 802.1x re-authentication disable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show aaa config	Displays the global AAA parameter configuration for 802.1X sessions.

MIB Objects

```
alaAaaAuthConfig
   alaAaaOnexReAuthStatus
   alaAaaOnexReAuthIntrvl
   alaAaaOnexReAuthTrustRadStatus
```

aaa interim-interval

Configures the amount of time between each interim accounting update for any given session.

aaa {802.1x | mac | captive-portal} interim-interval *seconds* **[trust-radius {enable | disable}]**

Syntax Definitions

802.1x	Configures the interim interval value for 802.1X accounting sessions.
mac	Configures the interim interval value for MAC accounting sessions.
captive-portal	Configures the interim interval value for Captive Portal accounting sessions.
seconds	The amount of time between each interim accounting update. The valid range is 60–1200 seconds.
trust-radius enable	Directs the switch to use the Acct-Interim-Interval attribute value for the interim time interval. This attribute is returned from the RADIUS server in an Accept-Accept message.
trust-radius disable	Directs the switch to use the locally configured interim time interval value.

Defaults

By default, the accounting interim interval value is set to 600 seconds.

parameter	default
trust-radius enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the trust RADIUS option is enabled, the accounting interim interval value received from the RADIUS server overrides the locally configured value for the switch.
- When the accounting interim interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.

Examples

```
-> aaa 802.1x interim-interval 1200
-> aaa 802.1x interim-interval 1200 trust-radius enable
-> aaa 802.1x interim-interval 1200 trust-radius disable

-> aaa mac interim-interval 1200
-> aaa mac interim-interval 1200 trust-radius enable
-> aaa mac interim-interval 1200 trust-radius disable

-> aaa captive-portal interim-interval 1200
```

```
-> aaa captive-portal interim-interval 1200 trust-radius enable
-> aaa captive-portal interim-interval 1200 trust-radius disable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show aaa config	Displays the global AAA parameter configuration for device authentication and accounting sessions.

MIB Objects

```
alaAaaAuthConfig
   alaAaaOnexIntrmIntrvl
   alaAaaOnexIntmIntvlTrstRadSts
   alaAaaMacIntrmIntrvl
   alaAaaMacIntmIntvlTrstRadStatus
   alaAaaCpIntrmIntrvl
   alaAaaCpIntmIntvlTrstRadStatus
```

aaa session-timeout

Configures whether or not an authenticated user is automatically logged out of the network based on a session timeout value.

aaa {mac | captive-portal} session-timeout {enable | disable} [interval *seconds***] [trust-radius {enable | disable}]**

Syntax Definitions

mac	Configures the session timeout parameter for authenticated MAC users.
captive-portal	Configures the session timeout parameter for authenticated Captive Portal users.
session-timeout enable	Enables the session timeout timer for authenticated user sessions.
session-timeout disable	Disables the session timeout timer for authenticated user sessions.
seconds	The session timeout value. The valid range is 12000–86400 seconds.
trust-radius enable	Directs the switch to use the Session-Timeout attribute returned from the RADIUS server in an Accept-Accept message.
trust-radius disable	Directs the switch to use the locally configured timeout interval value.

Defaults

By default, the session timer is disabled for the switch.

parameter	default
seconds	43200 seconds (12 hours)
trust-radius enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The session timeout parameter is configurable only for MAC and Captive Portal authentication sessions. When 802.1x re-authentication is enabled, the session timeout is set to 43200 seconds by default.
- The timeout interval is triggered when the session timeout parameter is enabled for the switch.
- When the trust RADIUS option is enabled, the timeout interval value received from the RADIUS server overrides the locally configured value for the switch.
- When the session timeout interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- When the session timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed.

Examples

```
-> aaa mac session-timeout enable interval 13000
-> aaa mac session-timeout enable interval 14000 trust-radius enable
-> aaa mac session-timeout disable

-> aaa captive-portal session-timeout enable interval 13000
-> aaa captive-portal session-timeout enable interval 14000 trust-radius enable
-> aaa captive-portal session-timeout disable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show aaa config	Displays the global AAA parameter configuration for device authentication and accounting sessions.

MIB Objects

```
alaAaaAuthConfig
   alaAaaMacSessTimeoutStatus
   alaAaaMacSessTimeoutIntrvl
   alaAaaMacSesTimeoutTrstRadStatus
   alaAaaCpSessTimeoutStatus
   alaAaaCpSessTimeoutIntrvl
   alaAaaCpSsTmotTrstRadStatus
```

aaa session console

Enables or disables switch access through the console port of the switch.

aaa session console {enable | disable}

Syntax Definitions

enable	Enables the switch access through the console port through the CLI shell.
disable	Disables the switch access through the console port through the CLI shell.

Defaults

parameter	default
enable | **disable**	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- It is recommended to create a back-up of the configuration file before using this command. Contact customer support to recover the switch.
- Before disabling the CLI console shell, configuration for telnet or SSH access with proper user privilege must be made.
- When the CLI console shell is disabled, the switch log output to the console is also disabled.
- When the CLI console shell is disabled, the switch can be accessed through SSH or telnet or WebView session.
- The command can be stored to the configuration file using **write memory**.
- If the console access is disabled through configuration (on both working and certified directory) and the telnet/SSH/WebView session is also not available to the switch, contact customer support to recover the switch.

Note. Deleting the configuration file will also delete the other configurations. Hence, it is recommended to create a back-up of the configuration file before deleting the configuration file.

- In a virtual chassis, the command must be used only on the master chassis; the console on master and all slaves will be disabled/enabled accordingly.

Examples

```
-> session console disable
-> session console enable
```

Release History

Release 8.6R2; command introduced.

Related Commands

show aaa session console config	Displays Session Manager information, such as banner file name, session timeout value, and default prompt value.

MIB Objects

```
alaAaaConsoleAccessConfig
   alaAaaConsoleAccessAdminState
```

aaa inactivity-logout

Configures whether or not an authenticated user is automatically logged out of the network after a specific period of inactivity.

aaa {mac | captive-portal} inactivity-logout {enable | disable} [interval *seconds***]**

Syntax Definitions

mac	Configures the inactivity logout timer for authenticated MAC users.
captive-portal	Configures the inactivity logout timer for authenticated Captive Portal users.
enable	Enables the inactivity logout timer for the specified authentication type.
disable	Disables the inactivity logout timer for the specified authentication type.
seconds	The inactivity logout time. The valid range is 60–1200 seconds, or enter 0 to indicate that an authenticated user should never be logged out.

Defaults

By default, the inactivity logout timer is disabled for the switch.

parameter	default
seconds	600 seconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The inactivity logout timer is configurable only for MAC and Captive Portal authentication sessions.
- The timer is triggered when the inactivity logout parameter is enabled for the switch.
- Make sure the configured inactivity logout time is set to a value greater than the MAC address aging time for the switch.
- If a specific time is configured for the inactivity logout timer, the user is *not* logged out of the network even if the MAC address for the user device ages out before the inactivity logout timer value expires.
- Setting the inactivity logout time to zero helps prevent silent devices from getting automatically logged out; the silent device will always remain logged in.
- When the inactivity logout time is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- If a user undergoes MAC authentication and then secondary Captive Portal authentication, the higher of the two inactivity logout timer values is applied to the device.

Examples

```
-> aaa mac inactivity-logout enable
-> aaa mac inactivity-logout enable interval 600
-> aaa mac inactivity-logout enable interval 0
-> aaa mac inactivity-logout disable

-> aaa captive-portal inactivity-logout enable
-> aaa captive-portal inactivity-logout enable interval 600
-> aaa captive-portal inactivity-logout enable interval 0
-> aaa captive-portal inactivity-logout disable
```

Release History

Release 8.1.1; command was introduced.
Release 8.4.1.R02; setting the inactivity logout time to zero is supported (user is never logged out).

Related Commands

show aaa config	Displays the global AAA parameter configuration for device authentication and accounting sessions.

MIB Objects

```
alaAaaAuthConfig
   alaAaaMacInActLogoutStatus
   alaAaaMacInActLogoutIntrvl
   alaAaaCpInActLogoutStatus
   alaAaaCpInActLogoutIntrvl
```

aaa radius nas-port-id

Configures the RADIUS client NAS-Port attribute for authentication and accounting sessions.

aaa radius nas-port-id {user-string *string* **| default}**

Syntax Definitions

string	A text string (up to 31 characters) used to define a NAS-Port identifier for the NAS-Port attribute.
default	Sets the NAS-Port attribute value to the chassis/slot/port of the user.

Defaults

By default, the NAS-Port attribute is set to the user port (chassis/slot/port).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The NAS-Port attribute value specified with this command is used in Account-Request messages and in Accounting-Request messages.

Examples

```
-> aaa radius nas-port-id default
-> aaa radius nas-port-id user-string nasport
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show aaa radius config	Displays the global RADIUS client attribute configuration.

MIB Objects

```
alaAaaClientAttrGroup
   alaAaaRadNasPortId
```

aaa radius nas-identifier

Configures the RADIUS client NAS-Identifier attribute for authentication and accounting sessions.

aaa radius nas-identifier {user-string *string* **| default}**

Syntax Definitions

string	A text string (up to 31 characters) used to identify the switch (RADIUS client) in the NAS-Identifier attribute.
default	Sets the NAS-Identifier attribute to the system name of the switch.

Defaults

By default, the NAS-Identifier attribute is set to the system name of the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The NAS-Identifier attribute value specified with this command is used in both Account-Request and Accounting-Request messages.

Examples

```
-> aaa radius nas-identifier default
-> aaa radius nas-identifier user-string os6860
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show aaa radius config	Displays the global RADIUS client attribute configuration.

MIB Objects

```
alaAaaClientAttrGroup
   alaAaaRadNasIdentifier
```

aaa radius nas-ip-address

Configure the RADIUS client NAS IP address attribute for the outgoing RADIUS packets.

aaa radius nas-ip-address {default | local-ip [*ip_address***]}**

Syntax Definitions

default	Sets the NAS IP address attribute value to the source IP address of the interface used to send the RADIUS packet. In OmniVista Cirrus it will be the VPN IP address.
local-ip	Sets the NAS IP address attribute value with the DHCP-Client interface IP address as the device identifier.
ip_address	The IPv4 address for NAS IP address attribute in RADIUS packets.

Defaults

By default, the value of NAS IP address is default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The NAS IP address attribute value configured will be used in all Authentication-Request messages and in Accounting-Request messages.
- If the Local IP is configured without the optional IP address, then the NAS IP address attribute value will be the DHCP-Client interface IP address.
- If there is no DHCP IP address configured on the switch, then NAS IP address attribute will contain the IP address as per the default behavior.
- If Local IP option is configured with an IP address, then this configured IP address value will be used in the NAS IP address attribute.

Examples

```
-> aaa radius nas-ip-address default
-> aaa radius nas-ip-address local-ip
-> aaa radius nas-ip-address local-ip 12.12.12.12
```

Release History

Release 8.5R4; command was introduced.

Related Commands

show aaa radius config	Displays the global AAA attribute values.

MIB Objects

```
alaAaaClientAttrGroup
   alaAaaRadNasIpAddressMode
   alaAaaRadNasIpAddressType
   alaAaaRadNasIpAddress
```

aaa radius mac-format

Configures the MAC address format to use in the specified RADIUS client attributes.

aaa radius mac-format {username | password | calling-station-id | called-station-id} delimiter {*char* **| none} case {uppercase | lowercase}**

Syntax Definitions

username	Configures the MAC address format for the User-Name attribute.
password	Configures the MAC address format for the User-Password attribute.
calling-station-id	Configures the MAC address format for the Calling-Station-Id attribute.
called-station-id	Configures the MAC address format for the Called-Station-Id attribute.
char	The delimiter character to use to separate the octets within a MAC address. The valid characters are a space (“ “), a hyphen (“-”), or a colon (“:”). For example, “e8 e7 32 a4 63 23”, “e8-e7-32-a4-63-23”, or “e8:e7:32:a4:63:23”.
none	No delimiter is used in the MAC address format.
uppercase	Uses uppercase characters in the MAC address format.
lowercase	Uses lowercase characters in the MAC address format.

Defaults

By default, no delimiter is used and the MAC address characters are in uppercase.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The MAC address format configured for the User-Name and User-Password attributes is only applied for MAC authentication and accounting, where these attributes are set to the MAC address of the user. The configured format is not applied for 802.1X or Captive Portal authentication and accounting.
- The MAC address format configured for the Called-Station-Id and Calling-Station-Id attributes is applied for MAC, 802.1X, and Captive Portal authentication and accounting sessions when these attributes are set to a MAC address value.
- The Called-Station-Id attribute is set to the base MAC address of the switch.
- The Calling-Station-ID attribute is configurable and can be set to the MAC address or IP address of the user.

Examples

```
-> aaa radius mac-format username delimiter none case lowercase
-> aaa radius mac-format username delimiter ":" case lowercase

-> aaa radius mac-format password delimiter none case lowercase
-> aaa radius mac-format password delimiter ":" case lowercase
```

```
-> aaa radius mac-format calling-station-id delimiter none case lowercase
-> aaa radius mac-format calling-station-id delimiter ":" case lowercase

-> aaa radius mac-format called-station-id delimiter none case lowercase
-> aaa radius mac-format called-station-id delimiter ":" case lowercase
```

Release History

Release 8.1.1; command was introduced.

Related Commands

aaa accounting radius calling-station-id	Sets the Calling-Station-Id attribute to the MAC address or IP address of the user for accounting sessions.
show aaa radius config	Displays the global RADIUS client attribute configuration.

MIB Objects

```
alaAaaRadiusClientGlobalAttr
   alaAaaRadiusUserNameDelimiter
   alaAaaRadiusUserNameCase
   alaAaaRadiusPasswordDelimiter
   alaAaaRadiusPasswordCase
   alaAaaRadCallnStnIdDelim
   alaAaaRadiusCallingStationIdCase
   alaAaaRadCalldStnIdDelim
   alaAaaRadiusCalledStationIdCase
```

aaa profile

Configures an AAA profile that is used to define and apply specific AAA parameter values to Universal Network Profile (UNP) Edge ports, link aggregates, or an Access Guardian Captive Portal profile. This section describes the base command (**aaa profile** *profile_name*) along with the other command keywords that are used to configure AAA parameter values that are applied when the profile is assigned to a UNP port or link aggregate.

aaa profile *profile_name*
[device-authentication {802.1x | mac | captive-portal} *server1* **[***server2***] [***server3***] [***server4***]]**
[accounting {802.1x | mac | captive-portal} {*server1* **[***server2***...] | syslog** *ip_address*
[port *udp_port***]}]**
[accounting {802.1x | mac | captive-portal} radius calling-station-id {mac-address | ip-address}]
[802.1x re-authentication {enable | disable} [interval *seconds***] [trust-radius {enable | disable}]]**
[{802.1x | mac | captive-portal} interim-interval *seconds* **[trust-radius {enable | disable}]]**
[{mac | captive-portal} session-timeout {enable | disable} [interval *seconds***] [trust-radius {enable | disable}]]**
[{mac | captive-portal} inactivity-logout {enable | disable} [interval *seconds***]]**
[radius nas-port-id {user-string *string* **| default}]**
[radius nas-identifier {user-string *string* **| default}]**
[radius nas-ip-address {default | local-ip [*ip_address***]}]**
[radius mac-format {username | password | calling-station-id | called-station-id} delimiter {*char* **| none} case {uppercase | lowercase}]**

no aaa profile *profile_name*

Syntax Definitions

profile_name	The name to associate with the AAA configuration profile.

Defaults

The AAA profile parameters are set to the same default values that are set when the explicit AAA command is used to configure the parameter value. See the **show aaa profile** command output example in the “Examples” section of this command page to determine default values for AAA profile parameters.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the AAA profile from the switch configuration.
- Creating the template name with the base command (**aaa profile** *profile_name*) is required before attempting to configure profile parameter values.
- When an AAA profile is assigned to a UNP port, the parameter values defined in the profile will override any existing global AAA configuration for users authenticating on that port.

- When an AAA profile is assigned to a Captive Portal profile, the parameters values defined in the AAA profile will override any existing global AAA configuration for users authenticated through the Captive Portal profile configuration.
- For more information about specific AAA parameter values, refer to the following explicit AAA configuration commands for each profile parameter option:

AAA Profile Parameter	Explicit Port Configuration Command
[device-authentication {802.1x | mac | captive-portal} *server1* [*server2*] [*server3*] [*server4*]]	**aaa device-authentication**
[accounting {802.1x | mac | captive-portal} {*server1* [*server2*...] | **syslog** *ip_address* [**port** *udp_port*]}]	**aaa accounting**
[accounting {802.1x | mac | captive-portal} radius calling-station-id {mac-address | ip-address}]	**aaa accounting radius calling-station-id**
[802.1x re-authentication {enable | disable} [interval *seconds*] [trust-radius {enable | disable}]]	**aaa 802.1x re-authentication**
[{802.1x | mac | captive-portal} interim-interval *seconds* [trust-radius {enable | disable}]]	**aaa interim-interval**
[{mac | captive-portal} session-timeout {enable | disable} [interval *seconds***] [trust-radius {enable | disable}]]**	**aaa session-timeout**
[{mac | captive-portal} inactivity-logout {enable | disable} [interval *seconds*]]	**aaa inactivity-logout**
[radius nas-port-id {user-string *string* | **default}]**	**aaa radius nas-port-id**
[**radius nas-identifier {user-string** *string* | **default}]**	**aaa radius nas-identifier**
[radius nas-ip-address {default | local-ip [*ip_address*]}]	**aaa radius nas-ip-address**
[radius mac-format {username | password | calling-station-id | called-station-id} delimiter {*char* | none} case {uppercase | lowercase}]	**aaa radius mac-format**

Examples

```
-> aaa profile prof1
-> no aaa profile prof1

-> aaa profile ap-1 device-authentication mac rad1 rad2
-> aaa profile ap-1 device-authentication 802.1x serv1 serv2 serv3 serv4
-> aaa profile ap-2 device-authentication captive-portal rad3 rad4
-> no aaa profile ap-2 device-authentication captive-portal

-> aaa profile ap-1 accounting 802.1x rad1 rad2 rad3
-> aaa profile ap-1 accounting mac rad1 rad2
-> aaa profile ap-1 accounting captive-portal syslog 10.135.67.99 port 8000
-> no aaa profile ap-1 accounting captive-portal

-> aaa profile ap-1 802.1x re-authentication enable trust-radius enable
-> aaa profile ap-1 802.1x re-authentication enable interval 700
-> aaa profile ap-1 802.1x re-authentication interval 700 trust-radius disable
-> aaa profile ap-1 802.1x re-authentication disable
```

```
-> aaa profile ap-1 mac inactivity-logout enable
-> aaa profile ap-1 mac inactivity-logout enable interval 600
-> aaa profile ap-1 mac inactivity-logout disable

-> aaa profile ap-1 captive-portal inactivity-logout enable
-> aaa profile ap-1 captive-portal inactivity-logout enable interval 600
-> aaa profile ap-1 captive-portal inactivity-logout disable

-> aaa profile abc radius nas-ip-address default
-> aaa profile abc radius nas-ip-address local-ip
-> aaa profile abc radius nas-ip-address local-ip 192.168.1.1
```

The following **show aaa profile** command output example shows the default values applied when the AAA profile is created:

```
-> show aaa profile ap-2

AAA profile name = ap-2
Authentication type = mac
    Session Timeout:
      Status            = disable,
      Interval (sec)    = 43200,
      Trust Radius      = disable

    Inactivity Timeout:
      Status            = disable,
      Interval (sec)    = 600

    Accounting Interim:
      Interval (sec)    = 600,
      Trust Radius      = disable

Authentication type = 802.1x
    Re-Authentication Timeout:
      Status            = disable,
      Interval (sec)    = 3600,
      Trust Radius      = disable

    Accounting Interim:
      Interval (sec)    = 600,
      Trust Radius      = disable

Authentication type = captive-portal
    Session Timeout:
      Status            = disable,
      Interval (sec)    = 43200,
      Trust Radius      = disable

    Inactivity Timeout:
      Status            = disable,
      Interval (sec)    = 600

    Accounting Interim:
      Interval (sec)    = 600,
      Trust Radius      = disable

RADIUS client attributes:
  NAS port id       = default,
```

```
NAS identifier    = default,
NAS IP address    = default,
  MAC format delimiter:
    Username           = none, UserNameCase = uppercase,
    Password           = none, PasswordCase = uppercase,
    calling station id = none, ClgStaIdCase = uppercase,
    called station id  = none, CldStaIdCase = uppercase
```

Release History

Release 8.1.1; command was introduced.
Release 8.5R4; **radius nas-ip-address** parameter added.

Related Commands

unp aaa-profile	Assigns an AAA profile to a UNP Edge port.
captive-portal-profile	Assigns an AAA profile to a Captive Portal profile.
show aaa profile	Displays the AAA profile configuration.

MIB Objects

```
alaAaaProfTable
  alaAaaProfOnexReAuthSts
  alaAaaProfOnexReAuthIntrvl
  alaAaaProfOnexReAuthTrstRadSts
  alaAaaProfOnexIntrmIntrvl
  alaAaaProfOnexIntmItvlTstRadSts
  alaAaaProfMacIntrmIntrvl
  alaAaaProfMacIntmItvlTrstRadSts
  alaAaaProfMacSessTimeoutSts
  alaAaaProfMacSessTimeoutIntrvl
  alaAaaProfMacSessTmoutTrstRadSts
  alaAaaProfMacInActLogoutSts
  alaAaaProfMacInActLogoutIntrvl
  alaAaaProfCpSessTimeoutSts
  alaAaaProfCpSessTimeoutIntrvl
  alaAaaProfCpSessTmotTrstRadSts
  alaAaaProfCpInActLogoutSts
  alaAaaProfCpInActLogoutIntrvl
  alaAaaProfCpIntrmIntrvl
  alaAaaProfCpItrmIntlTrstRadSts
  alaAaaProfRadNasPortId
  alaAaaProfRadNasIdentifier
  alaAaaProfRadUserNameDelim
  alaAaaProfRadPasswrdDelim
  alaAaaProfRadCallnStnIdDelim
  alaAaaProfRadCalldStnIdDelim
  alaAaaProfRadUserNameCase
  alaAaaProfRadPasswordCase
  alaAaaProfRadCallnStnIdCase
  alaAaaProfRadCalldStnIdCase
  alaAaaRadNasIpAddressMode
  alaAaaRadNasIpAddressType
  alaAaaRadNasIpAddress
```

user

Configures or modifies user entries in the local user database. Use the **no** form of the command to remove the user from the local database.

user *username*
{password *password* **| password-prompt}**
[expiration {*day* **|** *date***}]**
[read-only | read-write [*families...* | *domains...*| **all | none | all-except [***families* | *domains....***]]]**
[no snmp | no auth | sha | md5 | sha+des | md5+des | sha+aes | sha224 | sha256]
[console-only {enable | disable}]
[priv-password *password* **| prompt-priv-password]**

no user *username*

Syntax Definitions

username	The name of the user. Used for logging into the switch. Required to create a new user entry or for modifying a user. Maximum 63 characters.
password	The user's password in clear text or hexadecimal (corresponding to encrypted form). Required to create a new user entry. Maximum 30 characters.
password-prompt	This option allows to enter the password in a obscured format rather than as clear text. Select this option with the 'user' command to configure the password for the user. When this option is selected, a password prompt appears and the password can be provided. Password needs to be re-entered, and only if both the passwords match, command is accepted. The password provided in this mode is not displayed on the CLI as text.
day	The number of days before this user's current password expires. The range is 1 to 150 days.
date	The date (in the format *mm/dd/yyyy hh:mm*) that the user's current password will expire.
read-only	Specifies that the user will have read-only access to the switch.
read-write	Specifies that the user will have read-write access to the switch.
families	Determines the command families available to the user on the switch. Each command family should be separated by a space. Command families are subsets of domains.
domains	Determines the command domains available to the user on the switch. Each domain should be separated by a space.
all	Specifies that all command families and domains are available to the user.
none	Specifies that no command families or domains are available to the user.
all-except	Specifies that functional privileges for families or domains followed by 'all-except' are disabled to the user.
no snmp	Denies the specified user SNMP access to the switch.

no auth	Specifies that the user has SNMP access without any required SNMP authentication and encryption protocol.
sha	Specifies that the SHA authentication algorithm should be used for authenticating SNMP PDU for the user.
md5	Specifies that the MD5 authentication algorithm should be used for authenticating SNMP PDU for the user.
sha+des	Specifies that the SHA authentication algorithm and DES encryption standard should be used for authenticating and encrypting SNMP PDU for the user.
md5+des	Specifies that the MD5 authentication algorithm and the DES encryption standard should be used for authenticating and encrypting SNMP PDU for the user.
sha+aes	Specifies that the SHA authentication algorithm and AES encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha224	Specifies that the SHA224 authentication algorithm used for storing the user passwords.
sha256	Specifies that the SHA256 authentication algorithm used for storing the user passwords.
console-only enable	Enables console only access for the user *admin*.
console-only disable	Disables console only access for the user *admin*.
priv-password	Separate password that is used for SNMPv3 encryption. (8-30 characters)
prompt-priv-password	This option allows to enter the privacy password in a obscured format rather than as clear text. When this option is selected, press the Enter key. Select this option with the 'user' command to configure the privacy password for the user. When this option is selected, a password prompt appears and the privacy password can be provided. Password needs to be re-entered, and only if both the passwords match, command is accepted. The password provided in this mode is not displayed on the CLI as text.

Defaults

- By default, if a user is created without indicating the read and write privileges and SNMP access, the user will be given privileges based on the *default user account*. The ***default*** user account may be modified.
- By default, the password will be encrypted using SHA for all non SNMP users.
- For SNMP users without authentication, password will be encrypted with SHA.
- For SNMP users with authentication, it will be encrypted with the authentication method set for the user. If user is created with MD5, then it will be still encrypted with MD5.
- Users created with SHA2 authentication algorithm cannot be used for SNMP authentication.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- At least one user with SHA/MD5 authentication and/or DES encryption must be configured on the switch for SNMPv3 communication with OmniVista.
- Note that the exclamation point '!' is not a valid password character. In addition, specifying an asterisk (*) as one or more characters in a password is allowed as long as every character is not an asterisk. For example, **password **123456**** is allowed; **password ********** is not allowed.
- Some special characters are interpreted as a Linux shell variable by the switch when being used in a password. They can still be used in a password but they must be escaped ('\'). For example, to use the '$' as part of a password the following should be entered:

  ```
  -> user test password test\$1234
  ```

  this password will be interpreted as ***test$1234***.
- An alternative method is to use the **password-prompt** parameter when using special characters in a password. The **password-prompt** parameter exits the Linux shell and special characters are no longer interpreted as shell variables. The following characters are the majority of characters considered special characters by the switch [" " (white space), $, "", \,#, [], > <, |, ; , {}, (), ~, `].
- A password expiration for the user's current password may be configured with the **expiration** option. However, if the password is changed, or the global password expiration setting is configured with the **user password-expiration** command, the user's password expiration will be configured with the global expiration setting.
- When modifying a user's SNMP access, the user password must be re-entered (or a new one configured). This is required because the hash algorithm used to save the password in the switch depends on the SNMP authentication level.
- At initial startup, the default user on the switch is **admin** with a password of **switch**. The switch will not recreate this user at any successive startup as long as there exists at least one user defined with write access to all commands. (Note that if password expiration is configured for the **admin** user, or configured globally through the **user password-expiration** command, when the **admin** user's password expires, the **admin** user will have access only through the console port.)
- New users or updated user settings are saved *automatically*.
- The priv-password token is accepted only when SNMP level with encryption is configured for the user. If SNMP level with encryption is not selected and **priv-password** is configured, then CLI command is rejected with error.
- If priv-password is not configured for the user with encryption SNMP level, then the user password parameter is used for priv-password (both for authentication/encryption).
- Password policy is not applicable for the new optional parameter **priv-password**.
- For authenticating switch access through other access types such as telnet, FTP, SSH the existing user password will be used irrespective of whether **priv-password** is configured or not.
- When the SNMP level for an existing user with priv-password configured is changed from one encryption level to another encryption level, then the previously configured priv-password will not be used with the new SNMP level. Priv-password needs to be configured again when SNMP level is changed for an existing user.

Examples

```
-> user techpubs password writer_pass read-only config
-> user techpubs password-prompt
Enter Password: *******
Confirm Password: ********

-> user techpubs password writer_pass read-write all sha256
```

The following example creates a user with read-write privileges for all families except aaa.

```
-> user techpubs password writer_pass read-write all-except aaa

-> no user techpubs

-> user snmpv3user password pass1pass1 priv-password priv1priv1 read-write all
sha+aes

-> user snmpv3user password pass1pass1 prompt-priv-password
Enter Priv-Password: *********
Confirm Priv-Password: *********
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **password-prompt**, **all-except**, **priv-password**, **prompt-priv-password** parameter added, **sha224** and **sha256** algorithm support added.

Related Commands

password	Configures the current user's password.
show user	Displays information about users configured in the local database on the switch.

MIB Objects

```
aaaUserTable
   aaauPassword
   aaauReadRight
   aaauWriteRight
   aaauSnmpLevel
   aaauSnmpAuthKey
   aaauPasswordExpirationDate
```

password

Configures the current user's password.

password

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the **snapshot** command is used to capture the switch configuration, the text of the password is not displayed in the file. Instead an authentication key is included in the file.
- A new password cannot be identical to the current password; it cannot be identical to any of the three passwords that preceded the current password.
- Note that the exclamation point (!) is not a valid password character. In addition, specifying an asterisk (*) as one or more characters in a password is allowed as long as every character is not an asterisk. For example, **password** ****123456**** is allowed; **password ********** is not allowed.
- Password settings are saved *automatically*.

Examples

```
-> password
enter old password: ********
enter new password: *********
reenter new password: *********
->
```

Release History

Release 7.1.1; command was introduced.

Related Commands

user	Configures entries in the local user database. May be used by a system administrator to change any user's password in addition to configuring user privileges.

MIB Objects

```
aaaUserTable
   aaauPassword
   aaauOldPassword
```

user password-size min

Configures the minimum number of characters required when configuring a user password.

user password-size min *size*

Syntax Definitions

size	The number of characters required when configuring a user password through the **password** command or when setting up a user password through the **user** command. The range is 1 to 14 characters.

Defaults

parameter	default
size	6

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A.

Examples

```
-> user password-size min 9
```

Release History

Release 7.1.1; command was introduced.

Related Commands

user	Configures entries in the local user database. May be used by a system administrator to change any user's password in addition to configuring user privileges.
show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordSizeMin
```

user password-expiration

Configures an expiration date for all user passwords stored locally on the switch or disables password expiration.

user password-expiration {*day* | **disable}**

Syntax Definitions

day	The number of days before locally configured user passwords will expire. The range is 1 to 150 days.
disable	Disables password expiration for users configured locally on the switch.

Defaults

parameter	default
day | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **user password-expiration** command sets a default password expiration for users configured locally on the switch.
- Password expiration may be configured on a per-user basis through the **user** command; the user setting overrides the **user password-expiration** setting until the user password is changed or the **user password-expiration** command is entered again.

Examples

```
-> user password-expiration 2
-> user password-expiration disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

user	Configures entries in the local user database. May be used by a system administrator to change any user's password in addition to configuring user privileges.
show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaDefaultPasswordExpirationInDays
```

user password-policy cannot-contain-username

Specifies whether or not a user can configure a password that contains the username for the account.

user password-policy cannot-contain-username {enable | disable}

Syntax Definitions

enable	Does not allow the password to contain the username.
disable	Allows the password to contain the username.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The status of this function is specified as part of a global password policy that is applied to all passwords when they are created or modified.
- When this function is enabled, a check is done at the time the password is created or modified to ensure that the username is not specified as part of the password text.

Examples

```
-> user password-policy cannot-contain-username enable
-> user password-policy cannot-contain-username disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordContainUserName
```

user password-policy min-uppercase

Configures the minimum number of uppercase English characters required for a valid password.

user password-policy min-uppercase *number*

Syntax Definitions

number	The minimum number of uppercase characters. The valid range is 0–7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify **0** with this command to disable the minimum uppercase character requirement.
- The minimum number of uppercase characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-uppercase 2
-> user password-policy min-uppercase 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinUpperCase
```

user password-policy min-lowercase

Configures the minimum number of lowercase English characters required for a valid password.

user password-policy min-uppercase *number*

Syntax Definitions

number	The minimum number of uppercase characters. The valid range is 0–7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify **0** with this command to disable the minimum lowercase character requirement.
- The minimum number of lowercase characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-lowercase 2
-> user password-policy min-lowercase 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinLowerCase
```

user password-policy min-digit

Configures the minimum number of base-10 digits required for a valid password.

user password-policy min-digit *number*

Syntax Definitions

number	The minimum number of uppercase characters. The valid range is 0–7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify **0** with this command to disable the minimum number of digits requirement.
- The minimum number of digits requirement is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-digit 2
-> user password-policy min-digit 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinDigit
```

user password-policy min-nonalpha

Configures the minimum number of non-alphanumeric characters (symbols) required for a valid password.

user password-policy min-nonalpha *number*

Syntax Definitions

number	The minimum number of non-alphanumeric characters. The valid range is 0–7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify **0** with this command to disable the minimum non-alphanumeric character requirement.
- The minimum number of non-alphanumeric characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-nonalpha 2
-> user password-policy min-nonalpha 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinNonAlpha
```

user password-history

Configures the maximum number of old passwords to retain in the password history.

user password-history *number*

Syntax Definitions

number	The maximum number of old passwords to retain. The range is 0–24.

Defaults

parameter	default
number	4

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify **0** with this command to disable the password history function.
- The user is prevented from specifying any passwords that are recorded in the password history and fall within the range configured through this command.
- The password history value is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-history 2
-> user password-history 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordHistory
```

user password-min-age

Configures the minimum number of days during which a user is prevented from changing a password.

user password-min-age *days*

Syntax Definitions

days	The number of days to use as the minimum age of the password. The range is 0–150.

Defaults

parameter	default
days	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specify **0** with this command to disable the minimum number of days requirement.
- Configure the minimum age of a password with a value that is less than the value configured for the password expiration.
- The password minimum age value is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-min-age 7
-> user password-min-age 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy	Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordMinAge
```

user lockout-window

Configures a moving period of time (observation window) during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts. The number of failed login attempts is decremented by the number of failed attempts that age beyond the observation window time period.

user lockout-window *minutes*

Syntax Definitions

minutes	The number of minutes the observation window remains active. The range is 0–99999.

Defaults

parameter	default
minutes	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is only available to the **admin** user because the **admin** user account is the only account protected from any type of lockout attempt.
- Specify **0** with this command to disable the observation window function. This means that failed login attempts will never age out; the number of failed attempts is never decremented.
- Do not configure an observation window time period that is greater than the lockout duration time period.
- If the number of failed login attempts exceeds the number of failed attempts allowed before the observation window time expires, then the user account is locked out of the switch.
- The observation window time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved *automatically*.

Examples

```
-> user lockout-window 500
-> user lockout-window 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

user lockout-duration	Configures the amount of time a user account remains locked out of the switch.
user lockout-threshold	Configures the number of failed password attempts allowed before the user account is locked out of the switch.
user lockout unlock	Manually locks or unlocks a user account on the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaLockoutWindow
```

user lockout-threshold

Configures the number of failed password login attempts allowed during a certain period of time (observation window). If the number of failed attempts exceeds the lockout threshold number before the observation window period expires, the user account is locked out.

user lockout-threshold *number*

Syntax Definitions

number	The number of failed login attempts allowed. The range is 0–999.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is only available to the **admin** user because the **admin** user account is the only account protected from any type of lockout attempt.
- If the lockout threshold is set to zero (the default), there is no limit to the number of failed login attempts allowed.
- A user account remains locked out for the length of the lockout duration time period; at the end of this time, the account is automatically unlocked.
- If the lockout duration time period is set to zero, only the **admin** user or a user with read/write AAA privileges can unlock a locked user account. An account is unlocked by changing the user account password or with the **user lockout unlock** command.
- The lockout threshold time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved *automatically*; that is, these settings do not require the **write memory**, **reload slot**, or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-threshold 3
-> user lockout-threshold 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

user lockout-window	Configures a window of time during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts.
user lockout-duration	Configures the length of time a user account remains locked out of the switch.
user lockout unlock	Manually locks or unlocks a user account on the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaLockoutThreshold
```

user lockout-duration

Configures the length of time a user account remains locked out of the switch. At the end of this time period, the user account is automatically unlocked.

user lockout-duration *minutes*

Syntax Definitions

minutes	The number of minutes the user account remains locked out. The range is 0–99999.

Defaults

parameter	default
minutes	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is only available to the **admin** user because the **admin** user account is the only account protected from any type of lockout attempt.
- Note that if the lockout duration time period is set to zero (the default), then locked user accounts are never automatically unlocked.
- Only the **admin** user or a user with read/write AAA privileges can unlock a locked user account when the lockout duration time is set to zero. An account is unlocked by changing the user password or with the **user lockout unlock** command.
- Do not configure a lockout duration time period that is less than the amount of time configured for the observation window.
- The lockout duration time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved *automatically*; that is, these settings do not require the **write memory**, **reload slot**, or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-duration 60
-> user lockout-duration 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

user lockout-window	Configures a window of time during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts,
user lockout-threshold	Configures the number of failed password attempts allowed before the user account is locked out of the switch.
user lockout unlock	Manually locks or unlocks a user account on the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaLockoutDuration
```

user lockout unlock

Manually locks or unlocks a user account on the switch.

user *username* **{lockout | unlock}**

Syntax Definitions

username	The username of the account to lock or unlock.
lockout	Locks the user account out of the switch.
unlock	Unlocks a locked user account.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is only available to the **admin** user or a user with read/write AAA privileges.
- The **admin** user account is protected from any type of lockout attempt.
- User lockouts and unlocks are saved *automatically*.

Examples

```
-> user j_smith lockout
-> user j_smith unlock
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user	Displays information about all users or a particular user configured in the local user database on the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaUserTable
   aaauPasswordLockoutEnable
```

show aaa server

Displays information about a particular AAA server or AAA servers.

show aaa server [*server_name***]**

Syntax Definitions

server_name	The server name, which is defined through the **aaa radius-server, aaa tacacs+-server**, or **aaa ldap-server** commands.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If a server name is not included with this command, information for all of the servers is displayed.

Examples

```
-> show aaa server
Server name = ldap2
   Server type         = LDAP,
   Host name 1         = ors40535,
   Retry number        = 3,
   Timeout (sec)       = 2,
   Port                = 389,
   Domain name         = manager,
   Search base         = c=us,
   VRF                 = default
Server name = rad1
   Server type         = RADIUS,
   IP Address 1        = 10.10.2.1,
   IP Address 2        = 10.10.3.5,
   Retry number        = 3,
   Timeout (sec)       = 2,
   Authentication port = 1645,
   Accounting port     = 1646
   SSL enable          = TRUE,
   VRF                 = default
Health Check           = ENABLED,
Primary Server:
           Status      = DOWN,
           Uptime      = -,
           Downtime    = -,
           Down to UP transitions = 0,
Backup Server :
           Status      = DOWN,
           Uptime      = -,
           Downtime    = -,
```

```
           Down to UP transitions = 0
Server name = Tpub1
   Server type          = TACACS+,
   IP Address 1         = 10.10.5.1,
   Port                 = 3,
   Timeout (sec)        = 2,
   Encryption enabled   = no
   VRF                  = default

-> show aaa server rad1
Server name = rad1
   Server type         = RADIUS,
   IP Address 1        = 10.10.2.1,
   IP Address 2        = 10.10.3.5,
   Retry number        = 3,
   Timeout (sec)       = 2,
   Authentication port = 1645,
   Accounting port     = 1646
   SSL enable          = TRUE,
   VRF                 = default
Health Check           = ENABLED,
Primary Server:
           Status      = DOWN,
           Uptime      = -,
           Downtime    = -,
           Down to UP transitions = 0,
Backup Server :
           Status      = DOWN,
           Uptime      = -,
           Downtime    = -,
           Down to UP transitions = 0

-> show aaa server ldap2
Server name = ldap2
   Server type         = LDAP,
   Host name 1         = ors40535,
   Retry number        = 3,
   Timeout (in sec)    = 2,
   Port                = 389,
   Domain name         = manager,
   Search base         = c=us,
   VRF                 = default
```

output definitions

Server name	The name of the server. A RADIUS, TACACS+ or LDAP server name is defined through the **aaa radius-server, aaa tacacs+-server,** and **aaa ldap-server** commands respectively.
Server type	The type of server (LDAP, TACACS+, or RADIUS).
Host name	The name of the primary LDAP, TACACS+, or RADIUS host.
IP address	The IP address of the server.
Retry number	The number of retries the switch makes to authenticate a user before trying the backup server.
Timeout	The timeout for server replies to authentication requests.
Port	The port number for the primary LDAP or TACACS+ server.

output definitions

Encryption enabled	The status of the encryption.
Domain name	The super-user or administrative distinguished name in the format recognized by the LDAP-enabled directory servers.
Search base	The search base recognized by the LDAP-enabled directory servers.
Authentication port	The UDP destination port for authentication requests.
Accounting port	The UDP destination port for accounting requests.
SSL enable	The SSL enable field is displayed for the RADIUS server only when the SSL is enabled for RADIUS server.
VRF	Name of the VRF associated with the server.
Health Check	Whether a health check session is enabled or disabled for the RADIUS server.
Primary Server	The operational status, up time, down time, and the number of transitions from down to up for the primary RADIUS server. This field displays information gathered when RADIUS health check is enabled for the server.
Backup Server	The operational status, up time, down time, and the number of transitions from down to up for the back-up RADIUS server. This field displays information gathered when RADIUS health check is enabled for the server.

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **SSL enable** output field added for RADIUS server.
Release 8.5R4; **Health Check**, **Primary Server**, and **Backup Server** fields added for RADIUS server.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for Authenticated Switch Access.
aaa tacacs+-server	Configures or modifies an TACACS+ server for Authenticated Switch Access.
aaa radius-server health-check	Defines the RADIUS server health check configuration for a specific RADIUS server.
show aaa radius health-check-config	Displays the RADIUS server health check configuration.

MIB Objects

```
aaaServerTable
   aaasName
   aaasHostName
   aaasIpAddress
   aaasIpv6Address
   aaasHostName2
   aaasIpAddress2
   aaasIpv6Address2
   aaasRadKey
   aaasRetries
   aaasTimout
   aaasRadAuthPort
   aaasRadAcctPort
   aaasProtocol
   aaasTacacsKey
   aaasTacacsPort
   aaasLdapPort
   aaasLdapDn
   aaasLdapPasswd
   aaasLdapSearchBase
   aaasLdapServType
   aaasLdapEnableSsl
   aaasRadEnableSsl
   aaasVRFName
   aaasRadHealthCheck
```

show aaa server statistics

Displays the authorization, authentication, accounting, and BYOD statistics for the specified RADIUS server.

show aaa server *server_name* **statistics**

Syntax Definitions

server_name	The name of the RADIUS server for which statistics will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command applies only to RADIUS servers known to the switch (servers are identified through the **aaa radius-server** command).
- All statistics displayed for authorization, authentication, and accounting are displayed as an aggregate of the primary and back-up RADIUS server; separate statistics are not displayed for the primary server and the back-up server.
- Use the **aaa radius-server clear-statistics** command to reset all the statistics counters to zero.

Examples

```
-> show aaa server rad2 statistics
Statistics for rad2:
Authorization:
 Total No of Access-Request     : 2
 Total No of Access-Response    : 2
 Total No of Timedout Request   : 0
 Min RTT of Access Req/Res  usec: 938
 Avg RTT of Access Req/Res  usec: 1087
 Max RTT of Access Req/Res  usec: 1237
 Last RTT of Access Req/Res usec: 1237
Authentication:
 Total No of Access-Request     : 1
 Total No of Access-Response    : 1
 Total No of Access-Accept      : 1
 Total No of Access-Reject      : 0
 Total No of Access-Challenge   : 0
 Total No of Timedout Request   : 0
 Min RTT of Access Req/Res  usec: 1176
 Avg RTT of Access Req/Res  usec: 1176
 Max RTT of Access Req/Res  usec: 1176
 Last RTT of Access Req/Res usec: 1176
Accounting:
 Total No of Acct-Request       : 2
```

```
 Total No of Acct-Response      : 2
 Total No of Timedout Request   : 0
 Min RTT of Acct Req/Res    usec: 76657
 Avg RTT of Acct Req/Res    usec: 80182
 Max RTT of Acct Req/Res    usec: 83708
 Last RTT of Acct Req/Res   usec: 83708
BYOD:
 Total No of COA Request        : 0
 Total No of COA ACK Sent       : 0
 Total No of COA NACK Sent      : 0
 Total No of DM Request         : 0
 Total No of DM ACK Sent        : 0
 Total No of DM NACK Sent       : 0

Time of last statistics clear   : Thu Feb  1 18:09:06 2018

-> show aaa server auth-serv1 statistics
ERROR: Statistics are supported only for RADIUS servers
```

output definitions

Authorization	The statistics information displayed for authorization.
Total No of Access-Request	The total number of authorization access requests sent to the server.
Total No of Access-Response	The total number of authorization access responses received from the server.
Total No of Timedout Request	The total number of authorization access requests that timed out.
Min RTT of Access Req/Res	The minimum RTT of authorization access requests or responses for the last seven days.
Avg RTT of Access Req/Res	The average RTT of authorization access requests or responses for the last seven days.
Max RTT of Access Req/Res	The maximum RTT of authorization access requests or responses for the last seven days.
Last RTT of Access Req/Res	The last RTT of authorization access requests or responses.
Authentication	The statistics information displayed for authentication.
Total No of Access-Request	The total number of authentication access requests sent to the server.
Total No of Access-Response	The total number of authentication access responses received from the server.
Total No of Access-Accept	The total number of authentication access accepts received from the server.
Total No of Access-Reject	The total number of authentication access rejects received from the server.
Total No of Access-Challenge	The total number of authentication access challenges received from the server.
Total No of Timedout Request	The total number of authentication access requests that timed out.
Min RTT of Access Req/Res	The minimum RTT of authentication access requests or responses for the last seven days.
Avg RTT of Access Req/Res	The average RTT of authentication access requests or responses for the last seven days.

output definitions

Max RTT of Access Req/Res	The maximum RTT of authentication access requests or responses for the last seven days.
Last RTT of Access Req/Res	The last RTT of authentication access requests or responses.
Accounting	The statistics information displayed for accounting.
Total No of Acct -Request	The total number of accounting access requests sent to the server.
Total No of Acct -Response	The total number of accounting access responses received from the server.
Total No of Timedout Request	The total number of accounting access requests that timed out.
Min RTT of Acct Req/Res	The minimum RTT of accounting access requests or responses for the last seven days.
Avg RTT of Acct Req/Res	The average RTT of accounting access requests or responses for the last seven days.
Max RTT of Acct Req/Res	The maximum RTT of accounting access requests or responses for the last seven days.
Last RTT of Acct Req/Res	Displays the last RTT of accounting access requests or responses.
BYOD	Displays the BYOD statistics.
Total No of COA Request	The total number of Change of Authorization (CoA) requests received from the server.
Total No of COA ACK Sent	The total number of CoA-ACKs sent to the server.
Total No of COA NACK Sent	The total number of CoA-NACKs sent to the server.
Total No of DM Request	The total number of disconnect request messages received from the server.
Total No of DM ACK Sent	Displays the total number of disconnect ACKs sent to the server.
Total No of DM NACK Sent	Displays the total number of disconnect NACKs sent to the server.
Time of last statistics clear	The date and time the AAA statistics were last cleared for the server.

Release History

Release 8.5R4; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access.
aaa radius-server health-check	Enables or disables a RADIUS server health check.
aaa radius-server clear-statistics	Clears statistics collected for the specified RADIUS server.

MIB Objects

aaaAuthorServerStatsTable
- aaaAuthorStatsAccessReq
- aaaAuthorStatsAccessRes
- aaaAuthorStatsTimedOutReq
- aaaAuthorStatsCountRtt
- aaaAuthorStatsSumRtt
- aaaAuthorStatsMinRtt
- aaaAuthorStatsMaxRtt
- aaaAuthorStatsAvgRtt
- aaaAuthorStatsLastRtt

aaaAuthServerStatsTable
- aaaAuthStatsAccessReq
- aaaAuthStatsAccessRes
- aaaAuthStatsAccessAccept
- aaaAuthStatsAccessReject
- aaaAuthStatsAccessChal
- aaaAuthStatsTimedOutReq
- aaaAuthStatsCountRtt
- aaaAuthStatsSumRtt
- aaaAuthStatsMinRtt
- aaaAuthStatsMaxRtt
- aaaAuthStatsAvgRtt
- aaaAuthStatsLastRtt

aaaAcctServerStatsTable
- aaaAcctStatsAccessReq
- aaaAcctStatsAccessRes
- aaaAcctStatsTimedOutReq
- aaaAcctStatsCountRtt
- aaaAcctStatsSumRtt
- aaaAcctStatsMinRtt
- aaaAcctStatsMaxRtt
- aaaAcctStatsAvgRtt
- aaaAcctStatsLastRtt

aaaByodServerStatsTable
- aaaByodStatsCoaReq
- aaaByodStatsCoaAck
- aaaByodStatsCoaNack
- aaaByodStatsDmReq
- aaaByodStatsDmAck
- aaaByodStatsDmNack

aaa radius-server clear-statistics

Clears the AAA statistics collected for the specified RADIUS server.

aaa radius-server *server_name* **clear-statistics**

Syntax Definitions

server_name	The name of the RADIUS server on which the AAA statistics will be cleared.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **show aaa server statistics** command to display the statistics collected for the specified server.

Examples

```
-> aaa radius-server rad1 clear-statistics
-> aaa radius-server rad2 clear-statistics
```

Release History

Release 8.5R4; command introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access and device authentication.
aaa radius-server health-check	Enables or disables a RADIUS server health check with the specified parameters.
show aaa server statistics	Displays authorization, authentication, accounting, and BYOD statistics collected for a RADIUS server.

MIB Objects

```
aaaServerTable
   aaasHostName
   aaasClearStats
```

show aaa authentication

Displays information about the current authenticated switch session.

show aaa authentication

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **show aaa authentication** command to display authentication information about switch management services (Telnet, FTP, console port, Secure Shell, etc.).

Examples

```
-> show aaa authentication
Service type = Default
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = Console
   1rst authentication server  = local
Service type = Telnet
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = FTP
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = Http
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = Snmp
   Authentication = Use Default,
   1rst authentication server  = RadiusServer
   2nd authentication server   = local
Service type = Ssh
   Authentication = Use Default,
   1rst authentication server  = TacacsServer
   2nd authentication server   = local
```

output definitions

Authentication	Displays **denied** if the management interface is disabled. Displays **Use Default** if the management interface is configured to use the default configuration.
1st authentication server	The first server to be polled for authentication information.
2nd authentication server	The next server to be polled for authentication information.

Release History

Release 7.1.1; command was introduced.

Related Commands

aaa authentication	Configures the interface for Authenticated Switch Access and specifies the server(s) to be used.

MIB Objects

```
aaaAuthSATable
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
```

show aaa device-authentication

Displays a list of RADIUS servers assigned to provide 802.1X, MAC, or Captive Portal authentication.

show aaa device-authentication [802.1x | mac | captive-portal]

Syntax Definitions

802.1x	Displays the servers used for 802.1X authentication.
mac	Displays the servers used for MAC authentication.
captive-portal	Uses the servers used for Captive Portal authentication.

Defaults

By default, all assigned servers are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the optional **802.1x**, **mac**, or **captive-portal** parameters to display the servers assigned to provide the specified type of authentication.

Examples

```
-> show aaa device-authentication
Authentication type = mac
    Authentication Server:
      1st authentication server = cppm,
      2nd authentication server = rad1
      3rd authentication server = rad2,
      4th authentication server = rad3

Authentication type = 802.1x
    Authentication Server:
      1st authentication server = cppm,
      2nd authentication server = rad1

Authentication type = captive-portal
    Authentication Server:
      1st authentication server = cppm,
      2nd authentication server = rad1
```

output definitions

Authentication type	The type of authentication the server is assigned to provide (**802.1x**, **mac**, or **captive-portal**)
1st authentication server	The first server to be polled for authentication information. Any backup servers are also displayed on subsequent lines.

Release History

Release 7.2.1; command was introduced.
Release 7.3.4; **802.1x** and **mac** parameters added.
Release 8.1.1; **captive-portal** parameter added.

Related Commands

aaa device-authentication	Configures the RADIUS server to use for 802.1X or MAC authentication.

MIB Objects

```
AaaAuthMACTable
   aaaDaName1
   aaaDaName2
   aaaDaName3
   aaaDaName4
```

show aaa accounting

Displays information about accounting servers configured for authenticated switch access and device authentication sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

show aaa accounting [802.1x | mac | captive-portal]

Syntax Definitions

802.1x	Displays the RADIUS or syslog server used to log accounting for 802.1X authenticated sessions.
mac	Displays the RADIUS or syslog server used to log accounting for MAC authenticated sessions.
captive-portal	Displays the RADIUS or syslog server to log accounting for Captive Portal authenticated sessions.

Defaults

By default, the accounting server configuration is displayed for TACACS+ commands and management sessions (Telnet, FTP, console port, HTTP, or SNMP).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **802.1x**, **mac**, or **captive-portal** parameters to display the accounting server configuration for a specific type of device authentication.
- If no parameters are entered with this command, the accounting server configuration for authentication sessions and TACACS+ commands is displayed.

Examples

```
-> show aaa accounting mac
Accounting type = mac
    Accounting Server:
      1st Accnt Server = rad1,
      2nd Accnt Server = rad2

-> show aaa accounting 802.1x
Accounting type = 802.1x
    Syslog Accnt Server:
      IP Address = 135.254.163.110,
      UDP port   = 514

-> show aaa accounting captive-portal
Accounting type = captive-portal
    Syslog Accnt Server:
      IP Address = 135.254.163.110,
      UDP port   = 514
```

```
-> show aaa accounting
Session (telnet, ftp, ...)
  1st accounting server  = rad1
Command accounting server
  1st accounting server  = server1
```

Release History

Release 7.1.1; command was introduced.
Release 8.1.1; **802.1x**, **mac**, and **captive-portal** parameters added.

Related Commands

aaa accounting session	Configures an accounting server for authenticated switch access sessions.
aaa accounting command	Enables or disables the TACACS+ server for command accounting
aaa accounting	Configures RADIUS server accounting or local Switch Logging (syslog) accounting for device authentication sessions.

MIB Objects

```
aaaAcctDATable
   aaacdInterface
   aaacdName1
   aaacdName2
   aaacdName3
   aaacdName4
   aaacdSyslogIPAddrType
   aaacdSyslogIPAddr
   aaacdSyslogUdpPort
   aaacdRowStatus
```

show aaa config

Displays the AAA parameter configuration for 802.1X, MAC, and Captive Portal sessions.

show aaa {802.1x | mac | captive-portal} config

Syntax Definitions

802.1x	Displays the parameter configuration for 802.1X authenticated sessions.
mac	Displays the parameter configuration for MAC authenticated sessions.
captive-portal	Displays the parameter configuration for Captive Portal authenticated sessions.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **802.1x**, **mac**, or **captive-portal** parameters to display the parameter configuration for a specific type of device authentication.

Examples

```
-> show aaa 802.1x config
Authentication type = 802.1x
    Re-Authentication Timeout:
      Status                  = enable,
      Interval (sec)          = 3600,
      Trust Radius            = disable

    Accounting Interim:
      Interval (sec)          = 600,
      Trust Radius            = disable

-> show aaa mac config
Authentication type = mac
    Session Timeout:
      Status                  = disable,
      Interval (sec)          = 43200,
      Trust Radius            = disable

    Inactivity Timeout:
      Status                  = disable,
      Interval (sec)          = 600

    Accounting Interim:
      Interval (sec)          = 600,
      Trust Radius            = disable
```

```
-> show aaa captive-portal config
Authentication type = captive-portal
    Session Timeout:
      Status                  = disable,
      Interval (sec)          = 43200,
      Trust Radius            = disable

    Inactivity Timeout:
      Status                  = disable,
      Interval (sec)          = 600

    Accounting Interim:
      Interval (sec)          = 600,
      Trust Radius            = disable
```

output definitions

Authentication type	The type of authentication (**802.1x**, **mac**, or **captive-portal**).
Session Timeout	The parameter values for the AAA session timeout parameter. Does not apply to 802.1X authentication. Configured through the **aaa session-timeout** command.
Inactivity Logout	The parameter values for the AAA inactivity logout parameter. Does not apply to 802.1X authentication. Configured through the **aaa inactivity-logout** command.
Accounting Interim	The parameter values for the AAA accounting interim parameter. Configured through the **aaa interim-interval** command.
Re-authentication Timeout	The parameter values for the AAA 802.1X re-authentication timeout parameter. Does not apply to MAC or Captive Portal authentication. Configured through the **aaa 802.1x re-authentication** command.

Release History

Release 8.1.1; command was introduced.

Related Commands

show aaa device-authentication	Displays the device authentication server configuration.
show aaa accounting	Displays the accounting server configuration.
show aaa profile	Displays the AAA parameter profile configuration.

MIB Objects

```
alaAaaAuthConfig
   alaAaa8021XReAuthStatus
   alaAaa8021XReAuthIntrvl
   alaAaa8021XReAuthTrustRadStatus
   alaAaa8021XIntrmIntrvl
   alaAaa8021XIntmIntvlTrstRadStus
   alaAaaMacIntrmIntrvl
   alaAaaMacIntmIntvlTrstRadStatus
   alaAaaMacSessTimeoutStatus
   alaAaaMacSessTimeoutIntrvl
   alaAaaMacSesTimeoutTrstRadStatus
   alaAaaMacInActLogoutStatus
   alaAaaMacInActLogoutIntrvl
   alaAaaCpIntrmIntrvl
   alaAaaCpIntmIntvlTrstRadStatus
   alaAaaCpSessTimeoutStatus
   alaAaaCpSessTimeoutIntrvl
   alaAaaCpSsTmotTrstRadStatus
   alaAaaCpInActLogoutStatus
   alaAaaCpInActLogoutIntrvl
```

show aaa radius config

Displays the global AAA attribute values and MAC address format.

show aaa radius config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The MAC address format determines the delimiter character used between MAC address octets and whether or not characters are in uppercase or lowercase. This format is applied only when the RADIUS attribute value is set to a MAC address.

Examples

```
-> show aaa radius config
RADIUS client attributes:
  NAS port id         = default,
  NAS identifier      = default
  NAS IP address      = default
    MAC format delimiter:
      Username            = none, UserNameCase = uppercase,
      Password            = none, PasswordCase = uppercase,
      calling station id  = none, ClgStaIdCase = uppercase,
      called station id   = none, CldStaIdCase = uppercase
Unp Profile Precedence = Filter-Id
```

output definitions

NAS port id	The RADIUS client NAS-Port attribute for authentication and accounting sessions.
NAS identifier	The RADIUS client NAS-Identifier attribute for authentication and accounting sessions.
NAS IP address	The RADIUS client NAS-IP address attribute for authentication and accounting sessions.
MAC format delimiter	The MAC address format used in the specified RADIUS client attributes.
UNP Profile Precedence	The UNP profile precedence: **Filter-ID** or **Tunnel-Private-Group-ID**

Release History

Release 8.1.1; command was introduced.
Release 8.5R4; UNP Profile Precedence and NAS IP address field added.

Related Commands

show aaa device-authentication	Displays the device authentication server configuration.
show aaa accounting	Displays the accounting server configuration.
show aaa profile	Displays the AAA parameter profile configuration.
aaa radius nas-ip-address	Configure the RADIUS client NAS IP address attribute for the outgoing RADIUS packets.

MIB Objects

```
alaAaaAuthConfig
   alaAaa8021XReAuthStatus
   alaAaa8021XReAuthIntrvl
   alaAaa8021XReAuthTrustRadStatus
   alaAaa8021XIntrmIntrvl
   alaAaa8021XIntmIntvlTrstRadStus
   alaAaaMacIntrmIntrvl
   alaAaaMacIntmIntvlTrstRadStatus
   alaAaaMacSessTimeoutStatus
   alaAaaMacSessTimeoutIntrvl
   alaAaaMacSesTimeoutTrstRadStatus
   alaAaaMacInActLogoutStatus
   alaAaaMacInActLogoutIntrvl
   alaAaaCpIntrmIntrvl
   alaAaaCpIntmIntvlTrstRadStatus
   alaAaaCpSessTimeoutStatus
   alaAaaCpSessTimeoutIntrvl
   alaAaaCpSsTmotTrstRadStatus
   alaAaaCpInActLogoutStatus
   alaAaaCpInActLogoutIntrvl
```

show aaa radius health-check-config

Displays the RADIUS server health check configuration for each RADIUS server.

show aaa radius health-chec-config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the health check configuration for all RADIUS servers defined on the switch.

Examples

```
-> show aaa radius health-check-config
 Server                Health     Polling    Failover     Username
 Name                  Check      Interval   Status
--------------------+----------+----------+----------+-----------------------
RAD1                 DISABLED   60         DISABLED  alcatel
RAD2                 ENABLED    90         ENABLED   alcatel
```

output definitions

Server Name	The name of the RADIUS server.
Health Check	The operational status of the RADIUS health check feature for the server.
Polling Interval	The configured polling interval for the RADIUS server.
Failover Status	The status of the failover operation. When enabled, the re-authentication of users assigned to the authentication server down profile is triggered when the RADIUS server comes back up before the authentication server down timeout value expires).
Username	The configured user name for RADIUS server polling.

Release History

Release 8.5R4; command was introduced.

Related Commands

aaa radius-server health-check	Configures RADIUS health check for the specified RADIUS server.

MIB Objects

```
aaaServerTable
   aaasHostName
   aaasRadHealthCheck
   aaasRadPollingInterval
   aaasRadFailover
   aaasRadUsername
```

show aaa profile

Displays the AAA profile configuration.

show aaa profile [*profie_name***]**

Syntax Definitions

profile_name	The name of an existing AAA profile.

Defaults

By default, all profiles are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enter an AAA profile name with this command to display information about a specific profile.

Examples

```
-> show aaa profile ap2

AAA profile name = ap2
Authentication type = mac
    Authentication Server:
      1st Auth Server   = rad1,
      2nd Auth Server   = rad2

    Accounting Server:
      1st Accnt Server  = rad1,
      2nd Accnt Server  = rad2

    Session Timeout:
      Status            = disable,
      Interval (sec)    = 43200,
      Trust Radius      = disable

    Inactivity Timeout:
      Status            = disable,
      Interval (sec)    = 600

    Accounting Interim:
      Interval (sec)    = 600,
      Trust Radius      = disable

Authentication type = 802.1x
    Re-Authentication Timeout:
      Status            = disable,
      Interval (sec)    = 3600,
      Trust Radius      = disable
```

```
    Accounting Interim:
      Interval (sec)    = 600,
      Trust Radius      = disable

Authentication type = captive-portal
    Session Timeout:
      Status            = disable,
      Interval (sec)    = 43200,
      Trust Radius      = disable

    Inactivity Timeout:
      Status            = disable,
      Interval (sec)    = 600

    Accounting Interim:
      Interval (sec)    = 600,
      Trust Radius      = disable

RADIUS client attributes:
  NAS port id       = default,
  NAS identifier    = default,
  NAS ip address  = default,
    MAC format delimiter:
      Username           = none, UserNameCase = uppercase,
      Password           = none, PasswordCase = uppercase,
      calling station id = none, ClgStaIdCase = uppercase,
      called station id  = none, CldStaIdCase = uppercase
```

output definitions

Authentication type	The type of authentication (**802.1x**, **mac**, or **captive-portal**) configured through the profile.
Session Timeout	The profile values defined for the AAA session timeout parameter. Does not apply to 802.1X authentication.
Inactivity Logout	The profile values defined for the AAA inactivity logout parameter. Does not apply to 802.1X authentication.
Accounting Interim	The profile values defined for the AAA accounting interim parameter.
Re-authentication Timeout	The profile values defined for the AAA re-authentication timeout parameter. Does not apply to MAC or Captive Portal authentication.
RADIUS client attributes	The profile values defined for the NAS-Port, NAS-Port-Identifier and the NAS-IP address attributes and the format to use when the specified attribute value is set to a MAC address.

Release History

Release 8.1.1; command was introduced.
Release 8.5R4; **NAS IP address** output field added.

Related Commands

aaa profile	Configures an AAA profile.

MIB Objects

```
alaAaaProfTable
  alaAaaProfOnexReAuthSts
  alaAaaProfOnexReAuthIntrvl
  alaAaaProfOnexReAuthTrstRadSts
  alaAaaProfOnexIntrmIntrvl
  alaAaaProfOnexIntmItvlTstRadSts
  alaAaaProfMacIntrmIntrvl
  alaAaaProfMacIntmItvlTrstRadSts
  alaAaaProfMacSessTimeoutSts
  alaAaaProfMacSessTimeoutIntrvl
  alaAaaProfMacSessTmoutTrstRadSts
  alaAaaProfMacInActLogoutSts
  alaAaaProfMacInActLogoutIntrvl
  alaAaaProfCpSessTimeoutSts
  alaAaaProfCpSessTimeoutIntrvl
  alaAaaProfCpSessTmotTrstRadSts
  alaAaaProfCpInActLogoutSts
  alaAaaProfCpInActLogoutIntrvl
  alaAaaProfCpIntrmIntrvl
  alaAaaProfCpItrmIntlTrstRadSts
  alaAaaProfRadNasPortId
  alaAaaProfRadNasIdentifier
  alaAaaProfRadUserNameDelim
  alaAaaProfRadPasswrdDelim
  alaAaaProfRadCallnStnIdDelim
  alaAaaProfRadCalldStnIdDelim
  alaAaaProfRadUserNameCase
  alaAaaProfRadPasswordCase
  alaAaaProfRadCallnStnIdCase
  alaAaaProfRadCalldStnIdCase
```

show aaa session console config

Displays the current administrative state of the session console configuration.

show aaa session console config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show aaa session console config
Console access admin-state: disabled
```

Release History

Release 8.6R2; command introduced.

Related Commands

aaa session console	Enables or disables switch access through the console port of the switch

MIB Objects

N/A

show user

Displays information about all users or a particular user configured in the local user database on the switch.

show user [*username***]**

Syntax Definitions

username	The name of the user. Used for logging into the switch.

Defaults

By default, all users are displayed if the *username* parameter is not specified with this command.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display information about read/write access and partitioned management access (domains and families).

Examples

```
-> show user
User name = Customer1,
  Password expiration     = 10/27/2010 11:01 (30 days from now),
  Password allow to be modified date     = 9/30/2010 10:59 (3 days from now),
  Account lockout     = Yes (Automatically unlocked after 19 minute(s)from now),
  Password bad attempts     = 3,
  Read Only for domains   = None,
  Read/Write for domains  = Admin System Physical Layer2 Services policy Security ,
  Read/Write for families = ip rip ospf bgp vrrp ip-routing ipx ipmr ipms ,
  Snmp allowed     = YES,
  Snmp authentication     = SHA,
  Snmp encryption     = DES
User name = admin,
  Password expiration     = 10/27/2010 11:01 (30 days from now),
  Password allow to be modified date     = 9/30/2010 10:59 (3 days from now),
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = All ,
  Snmp allowed     = NO
```

output definitions

User name	The user name for this account.
Password expiration	The date and time on which the password will expire. This field only displays if the password expiration is configured specifically for a user, or a default password expiration is configured globally on the switch through the **user password-expiration** command. (Note that the date/time are based on the switch's default system date/time or the system date/time configured through the **system date** and **system time** commands.)
Password allow to be modified date	The earliest date and time on which the user may change the password. Configured through the **user password-min-age** command.
Account lockout	Indicates if the user account is locked out (**Yes** or **No**) and how many minutes remain until the user account is automatically unlocked. If no remaining time is displayed, the **admin** user or a user with admin privileges must manually unlock the account. Configured through the **user lockout-duration** and **user lockout unlock** commands.
Password bad attempts	The number of failed password login attempts for this user account.
Read Only for domains	The command domains available with the user's read-only access. See the table on the next page for a listing of valid domains.
Read/Write for domains	The command domains available with the user's read-write access. See the table on the next page for a listing of valid domains.
Read Only for families	The command families available with the user's read-only access. See the table on the next page for a listing of valid families.
Read/Write for families	The command families available with the user's read-write access. See the table on the next page for a listing of valid families.
Snmp allowed	Indicates whether or not the user is authorized to use SNMP (**YES** or **NO**). SNMP is allowed for the user account when SNMP authentication is specified for the account.
Snmp authentication	The level of SNMP authentication, if any, configured for the user. This field only displays if the user is authorized to use SNMP.
Snmp encryption	The level of SNMP encryption, if any, configured for the user. This field only displays if the user is authorized to use SNMP.

Possible values for command domains and families are listed here:

Domain	Corresponding Families
domain-admin	file telnet dshell debug
domain-system	system aip snmp rmon webmgt config
domain-physical	chassis module interface pmm health
domain-network	ip rip ospf bgp vrrp ip-routing ipx ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-policy	qos policy slb
domain-security	session avlan aaa

Release History

Release 7.1.1; command was introduced.

Related Commands

user	Configures user entries in the local user database.
show user password-policy	Displays the global password policy configuration for the switch.
show user lockout-setting	Displays the global user lockout settings for the switch.

MIB Objects

```
aaaUserTable
   aaauUserName
   aaauPasswordExpirationDate
   aaauPasswordExpirationInMinute
   aaauPasswordAllowModifyDate
   aaauPasswordLockoutEnable
   aaauBadAttempts
   aaauReadRight1
   aaauReadRight2
   aaauWriteRight1
   aaauWriteRight2
   aaauSnmpLevel
   aaauSnmpAuthkey
```

show user password-policy

Displays the global password settings configured for the switch.

show user password-policy

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The password policy contains parameter values that define configuration requirements for all passwords that are created on the switch. Use this command to display the current parameter values for the password policy.

Examples

```
-> show user password-policy
Password Policy:
Contain username flag: Enable
Minimum number of English uppercase characters: 6
Minimum number of English lowercase characters: 4
Minimum number of base-10 digit: 2
Minimum number of non-alphanumeric: 3
Minimum size: 8
Password history: 4
Password minimum age: 20 (days)
Password expiration: 40 (days)
```

output definitions

Contain username flag	Indicates if the username is included with the password check (**Enable** or **Disable**). Configured through the **user password-policy cannot-contain-username** command.
Minimum number of English uppercase characters	The minimum number of uppercase characters required in a password. Configured through the **user password-policy min-uppercase** command.
Minimum number of English lowercase characters	The minimum number of lowercase characters required in a password. Configured through the **user password-policy min-lowercase**.
Minimum number of base-10 digit	The minimum number of digits required in a password. Configured through the **user password-policy min-digit** command.

output definitions

Minimum number of non-alphanumeric	The minimum number of non-alphanumeric characters required in a password. Configured through the **user password-policy min-nonalpha** command.
Minimum size	The minimum number of characters required for the password size. Configured through the **user password-size min** command.
Password history	The maximum number of old passwords retained in the password history. Configured through the **user password-history** command.
Password minimum age	The number of days a password is protected from any modification. Configured through the **user password-min-age** command.
Password expiration	The default expiration date applied to all passwords. Configured through the **user password-expiration** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy	Displays the expiration date for passwords configured for user accounts stored on the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaPasswordContainUserName
   aaaAsaPasswordMinUpperCase
   aaaAsaPasswordMinLowerCase
   aaaAsaPasswordMinDigit
   aaaAsaPasswordMinNonAlpha
   aaaAsaPasswordHistory
   aaaAsaPasswordMinAge
   aaaAsaPasswordSizeMin
   aaaAsaDefaultPasswordExpirationInDays
```

show user lockout-setting

Displays the global user lockout settings for the switch.

show user lockout-setting

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The global lockout settings include parameter values that determine the length of a user observation window, the amount of time a locked user remains locked, and the number of failed password login attempts allowed.

Examples

```
-> show user lockout-setting
Lockout Setting:
Observation window: 30 (minutes)
Duration: 200 (minutes)
Threshold: 20
```

output definitions

Observation window	The amount of time, in minutes, during which the number of failed password login attempts are counted. Configured through the **user lockout-window** command.
Duration	The amount of time, in minutes, that a locked user account remains locked out of the switch. Configured through the **user lockout-duration** command.
Threshold	The maximum number of failed password login attempts allowed before the user is locked out of the switch. Configured through the **user lockout-threshold** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

user lockout unlock	Manually locks or unlocks a user account on the switch.
show user	Displays information about all users or a particular user configured in the local user database on the switch.

MIB Objects

```
aaaAsaConfig
   aaaAsaLockoutWindow
   aaaAsaLockoutDuration
   aaaAsaLockoutThreshold
```

show aaa priv hexa

Displays hexadecimal values for command domains/families. Useful for determining how to express command families in hexadecimal; hexadecimal values are used in configuring user privileges in attributes on an external LDAP or RADIUS authentication server.

show aaa priv hexa [*domain or family***]**

Syntax Definitions

domain or family	The CLI command domain or particular command family for which you want to display hexadecimal values. See table in Usage Guidelines.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Valid values for the family parameter are listed in the Corresponding Families column of the following table:

Domain	Corresponding Families
domain-admin	**file telnet dshell debug**
domain-system	**system aip snmp rmon webmgt config**
domain-physical	**chassis module interface pmm health**
domain-network	**ip rip ospf bgp vrrp ip-routing ipx ipmr ipms**
domain-layer2	**vlan bridge stp 802.1q linkagg ip-helper**
domain-service	**dns**
domain-policy	**qos policy slb**
domain-security	**session avlan aaa**

- Note that some command families may not be supported depending on the hardware platform you are running.
- If you do not specify a command family, hexadecimal values for all commands sets will display.

Examples

```
-> show aaa priv hexa
file            = 0x00000001 0x00000000,
telnet          = 0x00000008 0x00000000,
dshell          = 0x00000020 0x00000000,
debug           = 0x00000040 0x00000000,
domain-admin    = 0x00000069 0x00000000,

system          = 0x00000080 0x00000000,
aip             = 0x00000100 0x00000000,
snmp            = 0x00000200 0x00000000,
rmon            = 0x00000400 0x00000000,
webmgt          = 0x00000800 0x00000000,
config          = 0x00001000 0x00000000,
domain-system   = 0x00001F80 0x00000000,

chassis         = 0x00002000 0x00000000,
module          = 0x00004000 0x00000000,
interface       = 0x00008000 0x00000000,
pmm             = 0x00010000 0x00000000,
health          = 0x00040000 0x00000000,
domain-physical = 0x0005E000 0x00000000,

ip              = 0x00080000 0x00000000,
rip             = 0x00100000 0x00000000,
ospf            = 0x00200000 0x00000000,
bgp             = 0x00400000 0x00000000,
vrrp            = 0x00800000 0x00000000,
ip-routing      = 0x01000000 0x00000000,
ipx             = 0x02000000 0x00000000,
ipmr            = 0x04000000 0x00000000,
ipms            = 0x08000000 0x00000000,
domain-network  = 0x0FF80000 0x00000000,

vlan            = 0x10000000 0x00000000,
bridge          = 0x20000000 0x00000000,
stp             = 0x40000000 0x00000000,
802.1q          = 0x80000000 0x00000000,
linkagg         = 0x00000000 0x00000001,
ip-helper       = 0x00000000 0x00000002,
domain-layer2   = 0xF0000000 0x00000003,

dns             = 0x00000000 0x00000010,
domain-service  = 0x00000000 0x00000010,

qos             = 0x00000000 0x00000020,
policy          = 0x00000000 0x00000040,
slb             = 0x00000000 0x00000080,
domain-policy   = 0x00000000 0x000000E0,

session         = 0x00000000 0x00000100,
avlan           = 0x00000000 0x00000400,
aaa             = 0x00000000 0x00000800,
domain-security = 0x00000000 0x00000D00

-> show aaa priv hexa rip
0x00100000 0x00000000
```

Release History

Release 7.1.1; command was introduced.

Related Commands

user	Configures or modifies user entries in the local user database.

MIB Objects

N/A

show system fips

Displays the administrative and operational status of the FIPS mode on the switch.

show system fips

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The **show system fips** command is the only command that can be used to view the FIPS mode status. The FIPS status is not shown in the **show configuration snaphot** command output.

Examples

```
-> show system fips
Admin State: Enabled
Oper State: Enabled
```

Release History

Release 8.1.1; command introduced.

Related Commands

aaa authentication	Enable or disable the FIPS mode on the switch.

MIB Objects

```
systemFipsAdminState
   systemFipsOperState
```

aaa switch-access mode

Globally sets the access mode as enhanced or default.

aaa switch-access mode {default | enhanced}

Syntax Definitions

default	Sets the access mode as default.
enhanced	Sets the access mode as enhanced.

Defaults

parameter	default
default | enhanced	**default**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

It is recommended to save configuration and reboot the switch when the ASA access mode is configured.

Example

```
-> aaa switch-access mode default

-> aaa switch-access mode enhanced
WARNING: Recommended to save configuration and reload the switch upon switch access
mode change.
```

Release History

Release 8.3.1; command introduced.

Related Commands

show aaa switch-access mode	Displays the access mode configuration.

MIB Objects

```
aaaAsaConfig
   aaaAsaAccessMode
```

aaa switch-access ip-lockout-threshold

Configures the threshold value for failed login attempts from an IP address after which the IP address will be banned from switch access.

aaa switch-access ip-lockout-threshold *number*

Syntax Definitions

number	Set the threshold value for login attempts in the range 0 to 999.

Defaults

parameter	default
number	**6**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The command is applicable only if ASA enhanced mode is enabled.
- Set the IP threshold value to ‘0’ to disable the IP lockout thresholds.
- IP address is permanently blocked/banned if the number of authentication failures from a particular IP reaches IP lockout threshold limit within two times of the user lockout window.
- Only the switch access will be restricted from the banned IP address. Any IP packet (with monitored port number) destined to a switch IP interfaces will be discarded. IP packets normally bridged/routed by the switch will not be discarded.
- A maximum of 128 IP addresses can be added to the banned list. When the maximum limit has reached, oldest entry from the list is removed to accommodate the new entries.
- User lockout window (**user lockout-window)** is applicable for IP lockout threshold as well.
- IP lockout threshold shall share the same window as user lockout window, and by default, IP lockout threshold shall be two times that of user lockout window. Since user lockout is giving more priority, the IP lockout threshold must be greater than the user lockout threshold value.
- The IP address will remain blocked until it is released using the command **aaa switch-access banned-ip release**.

Example

```
-> aaa switch-access ip-lockout-threshold 2
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access mode	Globally sets the access mode as enhanced or default.
show aaa switch-access ip-lockout-threshold	Displays the lockout threshold configured for the remote IP addresses.

MIB Objects

```
aaaAsaConfig
   aaaAsaAccessIpLockoutThreshold
```

aaa switch-access banned-ip release

Releases the banned IP addresses that are blocked due to failed login attempts.

aaa switch-access banned-ip {all | *ip_address***} release**

Syntax Definitions

all	Release all banned IP addresses from the banned list.
ip_address	Release a specific IP address from the banned list.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The IP addresses are banned if the failed login count reaches IP lockout threshold limit.

Example

```
-> aaa switch-access banned-ip all release
-> aaa switch-access banned-ip 100.2.45.56 release
```

Release History

Release 8.3.1; command introduced.

Related Commands

show aaa switch-access banned-ip	Displays the list of banned ip addresses.

MIB Objects

```
aaaSwitchAccessBannedIpTable
   aaaSwitchAccessBannedIpAddress
   aaaSwitchAccessBannedIpRowStatus
```

aaa switch-access priv-mask

Configure the functional privileges mask for the switch access based on the access type on top of the user privilege.

aaa switch-access priv-mask {console | telnet | ssh | http | https} {read-only | read-write} [*families...* | *domains...*| **all | none | all-except** *families...***]**

Syntax Definitions

read-only	Specifies that the user will have read-only access to the switch through a specific access type.
read-write	Specifies that the user will have read-write access to the switch through a specific access type.
families	Determines the command families available to the user on the switch for a specific access type. Each command family should be separated by a space. Command families are subsets of domains. See *Usage Guidelines* for more details.
domains	Determines the command domains available to the user on the switch for a specific access type. Each domain should be separated by a space. See the Usage Guidelines for more details.
all	Specifies that all command families and domains are available to the user for a specific access type.
none	Specifies that no command families or domains are available to the user for a specific access type.
all-except	Specifies that functional privileges for families followed by 'all-except' are disabled for a specific access type.

Defaults

By default, the access types are enabled with read-write privileges for all the families.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The command is applicable only when ASA enhanced mode is enabled.
- The access privileges for the SSH, TELNET, Console, HTTP, HTTPS can be defined.
- Possible values for domains and families are listed in the table here:

Domain	Corresponding Families
domain-admin	file telnet debug
domain-system	system aip snmp rmon webmgt config
domain-physical	chassis module interface pmm health

domain-network	ip rip ospf bgp vrrp ip-routing ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-policy	qos policy slb
domain-security	session avlan aaa
domain-mpls	mpls
domain-datacenter	fips, auto-fabric
domain-afn	sip-snooping, dpi, app-mon

Example

```
-> aaa switch-access priv-mask ssh read-only webmgt vrrp vrf vlan udld
-> aaa switch-access priv-mask telnet read-write tftp-client telnet system stp ssh
-> aaa switch-access priv-mask ssh read-only all-except vlan
-> aaa switch-access priv-mask telnet read-write all-except ip
```

If privileges for specific families need to be applied, then remove the existing privilege using the **no** command, and re-apply the required family privilege.

```
-> no aaa switch-access priv-mask telnet read-write all
-> aaa switch-access priv-mask telnet read-write vlan aaa
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access mode	Globally sets the access mode as enhanced or default.
show aaa switch-access priv-mask	Displays the privilege details for the access types.

MIB Objects

```
aaaSwitchAccessPrivMaskTable
   aaaSwitchAccessType
   aaaSwitchAccessReadRight1
   aaaSwitchAccessReadRight2
   aaaSwitchAccessReadRight3
   aaaSwitchAccessReadRight4
   aaaSwitchAccessWriteRight1
   aaaSwitchAccessWriteRight2
   aaaSwitchAccessWriteRight3
   aaaSwitchAccessWriteRight4
```

aaa switch-access management-stations admin-state

Enables or disables the IP management station feature in a switch.

aaa switch-access management-stations admin-state {enable | disable}

Syntax Definitions

enable	Enables the IP management station feature in the switch.
disable	Disables the IP management station feature in the switch.

Defaults

The IP management station feature is disabled by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The command is applicable only when ASA enhanced mode is enabled.
- When the IP management station is disabled, switch access from any IP address shall be allowed. If there is a login failure (based on the **ip-lockout threshold** value), the IP address will be banned/ blocked and added to the banned IP address list.
- When the IP management station is enabled, the switch access will be allowed only from those IPs configured in the management station list and only if those are not in banned list.
- It is recommended to enable this command from console since this may terminate the existing session, if enabled through telnet or SSH.

Example

```
-> aaa switch-access management stations admin-state enable
-> aaa switch-access management stations admin-state disable
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access mode	Globally sets the access mode as enhanced or default.
aaa switch-access management-stations	Configure the management station in the switch, with or without mask value for the corresponding IP of the management station.
show aaa switch-access management-stations	Displays the list of configured management stations.

MIB Objects

```
aaaSwitchAccessMgmtStationTable
   aaaSwitchAccessMgmtStationRowStatus
```

aaa switch-access management-stations

Configure the management station in the switch, with or without mask value for the corresponding IP of the management station. The remote access is allowed only from these IP addresses if management station feature is enabled.

aaa switch-access management-stations [*ip_address* | *ip_address /mask***]**

no aaa switch-access management-stations *ip_address*

Syntax Definitions

ip_address	IP address and the mask of the management station.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The command is configurable when **aaa switch-access management-stations admin-state** is enabled.
- A maximum of 64 management stations can be configured.
- Removing an IP address from the management station list will not remove the IP from the banned list.
- Whenever an IP address is removed from the management station, switch will stop responding to that IP. However, the existing sessions are not terminated automatically.

Example

```
-> aaa switch-access management stations 100.15.9.8
-> aaa switch-access management stations 100.15.9.9 255.255.255.0
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access management-stations admin-state	Enables or disables the IP management station feature in a switch.
show aaa switch-access management-stations	Displays the list of configured management stations.

MIB Objects

```
aaaSwitchAccessMgmtStationTable
   aaaSwitchAccessMgmtStationIpAddress
```

show aaa switch-access mode

Displays the access mode configuration.

show aaa switch-access mode

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show aaa switch-access mode
AAA Switch Access:
  Switch Access Mode            = Default,
  Restricted Management Station = Disabled
```

output definitions

Switch Access Mode	ASA access mode: Enhanced or Default
Restricted Management Station	The status of the IP management station feature in a switch: Enabled or Disabled

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access mode	Globally sets the access mode as enhanced or default.

MIB Objects

```
aaaAsaConfig
   aaaAsaAccessMode
```

show aaa switch-access ip-lockout-threshold

Displays the IP lockout threshold value.

show aaa switch-access ip-lockout-threshold

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show aaa switch-access ip-lockout-threshold
ip Lockout Threshold = 6
```

output definitions

IP lockout threshold	The IP lockout threshold value.

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access ip-lockout-threshold	Configures the threshold for failed login attempts from an IP address after which the IP address will be banned from switch access.

MIB Objects

```
aaaAsaConfig
   aaaAsaAccessIpLockoutThreshold
```

show aaa switch-access banned-ip

Displays the list of banned IP addresses.

show aaa switch-access banned-ip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show aaa switch-access banned-ip
   S. No     Banned IP address
|---------+--------------------
     1       100.15.5.21
     2       100.15.5.22
```

output definitions

Banned IP address	The banned IP address blocked due to failed login attempts.

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access banned-ip release	Releases the banned IP addresses that are blocked due to failed login attempts.

MIB Objects

```
aaaSwitchAccessBannedIpTable
   aaaSwitchAccessBannedIpAddress
```

show aaa switch-access priv-mask

Displays the privilege details for the access types.

show aaa switch-access priv-mask

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show aaa switch-access priv-mask
Interface Type = CONSOLE,
  Read Only for domains   = All ,
  Read/Write for domains  = All
Interface Type = TELNET,
  Read Only for domains   = All ,
  Read/Write for domains  = All
Interface Type = SSH,
  Read Only for domains   = All ,
  Read/Write for domains  = All
Interface Type = HTTP,
  Read Only for domains   = All ,
  Read/Write for domains  = All
Interface Type = HTTPS,
  Read Only for domains   = All ,
  Read/Write for domains  = All
```

output definitions

Interface Type	The interface type.
Read Only for domains	Read-only privileges for the domains.
Read/Write for domains	Read-write privileges for the domains.

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access priv-mask	Configure the functional privileges for a particular access type.

MIB Objects

```
aaaSwitchAccessPrivMaskTable
   aaaSwitchAccessType
   aaaSwitchAccessReadRight1
   aaaSwitchAccessReadRight2
   aaaSwitchAccessReadRight3
   aaaSwitchAccessReadRight4
   aaaSwitchAccessWriteRight1
   aaaSwitchAccessWriteRight2
   aaaSwitchAccessWriteRight3
   aaaSwitchAccessWriteRight4
```

show aaa switch-access management-stations

Displays the list of configured management stations.

show aaa switch-access management-stations

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show aaa switch-access management-stations
AAA Switch Access:
Restricted Management station = ENABLED
   Management         Subnet
   IP Address         Prefix
-----------------+---------------
   100.15.5.21    255.255.255.255
```

output definitions

Restricted Management station	IP management station status: Enabled or disabled.
Management IP address	IP address of the management station.
Subnet Prefix	The prefix corresponding to the IP address.

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access management-stations admin-state	Enables or disables the IP management station feature in a switch.
aaa switch-access management-stations	Configure the management station in the switch, with or without mask value for the corresponding IP of the management station.

MIB Objects

```
aaaSwitchAccessMgmtStationTable
   aaaSwitchAccessMgmtStationRowStatus
   aaaSwitchAccessMgmtStationIpAddress
```

show aaa switch-access hardware-self-test

Displays the major hardware component status.

show aaa switch-access hardware-self-test

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The command is applicable only when ASA enhanced mode is enabled.

Examples

```
-> show aaa switch-access hardware-self-test
Checking CPU status -> Ok
Checking Memory status -> Ok
Checking Flash Status -> Ok
Checking NI Module status -> Ok
Checking Power Supply status -> Ok
Checking Lanpower Status -> Ok
Checking GBIC Status -> Ok
```

Release History

Release 8.3.1; command introduced.

Related Commands

show aaa switch-access process-self-test Displays the major software process status.

MIB Objects

N/A

show aaa switch-access process-self-test

Displays the major software process status.

show aaa switch-access process-self-test

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The command is applicable only when ASA enhanced mode is enabled.

Examples

```
-> show aaa switch-access process-self-test
------------+------------------
     Process Self Test
------------+------------------
Checking Chassis Supervision Process -> Ok
Checking AAA Process -> Ok
Checking Configuration Manager Process -> Ok
Checking Network Process -> Ok
Checking QoS Process ---> Ok
Checking VLAN Manager Process -> Ok
Checking H/W Driver Process -> Ok
Checking Layer2/Switching -> Ok
Checking Layer3/Switching -> Ok
```

Release History

Release 8.3.1; command introduced

Related Commands

show aaa switch-access hardware-self-test	Displays the major hardware components status.

MIB Objects

N/A

aaa common-criteria admin-state

Enables or disables common criteria mode on the switch.

aaa common-criteria admin-state {enable | disable}

Syntax Definitions

enable | disable Enables or disables the common criteria mode.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configuration is applied only after a reload of the switch.
- Please refer to the **Preparation and Operation of Common Criteria** guide available on the Service and Support website for additional information on Common Criteria implementation.

Examples

```
-> aaa common-criteria admin-state enable
WARNING: Common Criteria configuration is applied only after reload
```

Release History

Release 8.3.1; command introduced.

Related Commands

show aaa common-criteria config	Displays the common criteria status on the switch.

MIB Objects

N/A

show aaa common-criteria config

Displays the common criteria status on the switch.

show aaa common-criteria config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show aaa common-criteria config
Admin State: Enabled,
Operational State: Enabled
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa common-criteria admin-state	Enables or disables common criteria mode on the switch.

MIB Objects

N/A

aaa certificate update-ca-certificate

Updates the CA-bundle with the custom CA server certificate provided by CA.

aaa certificate update-ca-certificate *ca_file*

Syntax Definitions

ca_file	The custom CA server certificate (in PEM format) provided by the CA.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The custom CA server certificate should be copied in PEM format to the **/flash/switch/cert.d** directory via SFTP.
- This command appends the existing CA bundle (**certs.pem**) and the custom CA server certificate provided as input.
- The update of custom CA server certificates needs to be done before corresponding server configurations are done on the switch. If the update is done post server configuration, then a switch reboot needs to be done for the changes to take effect.

Examples

```
-> aaa certificate update-ca-certificate ca.pem
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa certificate update-crl	Updates the CRL list with the custom CRL provided by CA.

MIB Objects

N/A

aaa certificate update-crl

Updates the CRL list with the custom CRL provided by CA.

aaa certificate update-crl *crl_file*

Syntax Definitions

crl_file	The custom CRL file (in PEM format) provided by the CA.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The custom CRL file should be copied in PEM format to the **/flash/switch/cert.d** directory via SFTP.
- This command appends the existing CRL file (**crl.pem**) and the custom CRL provided as input.
- The update of the custom CRL needs to be done before corresponding server configurations are done on the switch. If the update is done post server configuration, then a switch reboot needs to be done for the changes to take effect.

Examples

```
-> aaa certificate update-crl crl.pem
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa certificate update-ca-certificate	Updates the CA-bundle with the custom CA server certificate provided by CA.

MIB Objects

N/A

aaa certificate generate-rsa-key key-file

Generates the RSA 2048 bit key with the file name provided as input.

aaa certificate generate-rsa-key key-file *key_file*

Syntax Definitions

key_file	The name of the key file under which the RSA 2048 bit key is stored.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Generates RSA 2048 bit key in **/flash/switch/cert.d** directory with the file name as the input key file.

Examples

```
-> aaa certificate generate-rsa-key key-file myCliPrivate.key
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa certificate generate-self-signed	Generates the X.509 self-signed certificate for TLS client authentication.
aaa certificate view	Displays the contents of the X.509 certificate.
aaa certificate delete	Deletes the X.509 certificate.

MIB Objects

N/A

aaa certificate generate-self-signed

Generates the X.509 self-signed certificate for TLS client authentication.

aaa certificate generate-self-signed {*cert_file***} key {***key_file***} [days** *valid_period***} {CN** *common_name***} {ON** *org_name***} {OU** *org_unit***} {L** *locality***} {ST** *state***} {C** *country***}**

Syntax Definitions

cert_file	The name of the X.509 certificate file to be created.
key_file	The name of the key file under which the RSA 2048 bit key is stored.
valid_period	Validity period (in days) of the X.509 certificate.
common_name	Common Name used in X.509 certificate.
org_name	The Organization Name used in X.509 certificate.
org_unit	The Organization Unit used in X.509 certificate.
locality	The Locality used in X.509 certificate.
state	The State used in X.509 certificate.
country	The Country used in X.509 certificate.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command generates the file in **/flash/switch/cert.d** directory.
- Default values will be taken for all other optional parameters while generating the X.509 certificate.
- The X.509 certificate needs to be done before corresponding server configurations are done on the switch. If the certificate is created post server configuration, then a switch reboot needs to be done for the changes to take effect.

Examples

```
-> aaa certificate generate-self-signed myCliCert.pem key clientkey.key days 3650
cn client.ale.com on ALE ou ESD l BAN st KAR c IN
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa certificate generate-rsa-key key-file	Generates the RSA 2048 bit key with the file name provided as input.
aaa certificate view	Displays the contents of the X.509 certificate.
aaa certificate delete	Deletes the X.509 certificate.

MIB Objects

N/A

aaa certificate view

Displays the contents of the X.509 certificate.

aaa certificate view *cert_file*

Syntax Definitions

cert_file	The X.509 certificate file (in PEM format) to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> aaa certificate view clientcert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:8f:11:63:23:d4:28:f6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=client.ale.com , O=ale , OU=esd , L=bn , ST=kar , C=in
        Validity
            Not Before: Jan  3 23:09:07 2014 GMT
            Not After : Jan  1 23:09:07 2024 GMT
        Subject: CN=client.ale.com , O=ale , OU=esd , L=bn , ST=kar , C=in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cc:72:7a:12:d3:66:16:8f:9f:22:59:d1:7a:05:
                    03:1f:bf:51:93:21:8d:95:74:18:88:78:71:62:1f:
                    09:04:2c:ce:dc:0a:2f:b6:88:76:ca:9d:1a:f4:73:
                    88:54:96:e8:84:95:81:3c:81:75:c4:47:db:44:a7:
                    aa:1a:75:5d:3d:b0:82:a5:7c:b8:5e:5d:f3:50:81:
                    1b:62:a1:04:2b:55:c4:2e:9b:8a:48:e0:3a:e0:be:
                    55:a3:3b:56:ca:5c:11:14:77:36:54:35:41:4e:40:
                    e6:8b:8c:50:2f:65:ad:da:04:f9:36:8d:8a:68:5f:
                    ba:a0:71:32:7b:fb:b8:95:3b:d0:bb:ac:d0:bd:db:
                    70:29:08:00:3a:96:5e:0c:f0:0f:45:0d:35:78:60:
                    05:0d:b2:d0:14:1d:08:2a:39:13:eb:6e:58:3b:09:
                    8b:ae:47:18:3e:22:25:2e:2a:91:a6:84:21:85:e4:
                    05:88:8b:bf:6b:6f:a5:0c:3f:17:94:a0:3f:56:d7:
                    f6:95:b6:33:ce:5b:7b:39:57:1d:62:e0:e7:8c:3e:
                    4f:64:ac:19:68:14:c3:af:ee:f2:fa:6e:70:c1:23:
```

```
                    10:0c:72:ad:a8:87:94:a8:99:52:db:b6:13:b4:ec:
                    5e:64:b9:89:1a:8a:ce:c3:db:db:5e:69:c0:4e:43:
                    22:5b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                64:09:19:62:F8:14:FE:ED:A5:B7:9F:C6:BA:8F:B0:30:3C:B2:7F:96
            X509v3 Authority Key Identifier:
                keyid:64:09:19:62:F8:14:FE:ED:A5:B7:9F:C6:BA:8F:B0:30:3C:B2:7F:96

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         48:d8:ad:86:06:61:c9:20:67:d0:b3:b2:67:87:b9:01:49:8f:
         8b:9b:df:5b:fd:b2:7c:1f:38:d1:e8:73:13:29:1a:68:7a:ae:
         d8:56:73:e8:48:06:d8:6a:7f:46:2b:08:fc:f4:fb:21:60:f6:
         b9:c9:13:93:71:1b:7f:9c:18:b0:ce:3f:12:b1:e6:b9:8f:ce:
         9f:4e:87:83:21:e2:be:0a:89:be:19:b3:16:14:e3:c0:b4:94:
         e7:12:c0:fe:c8:fe:2c:f0:0c:72:5c:6c:8f:17:b5:0d:25:e4:
         7e:12:1e:38:d7:5f:7b:0d:b2:aa:bb:d7:66:33:3f:49:ee:ef:
         14:c0:c2:d8:74:3c:1a:35:f4:3a:53:2a:1c:88:6b:e9:20:cb:
         72:b2:1a:83:0c:93:df:3d:75:c4:cb:c8:ab:57:1a:dc:13:bc:
         a9:d5:8d:64:2c:bb:56:3a:54:c4:e4:c3:77:85:3d:ff:21:f5:
         d8:48:35:e0:e5:07:d7:fd:04:7c:fe:d2:b8:3c:dd:38:e6:57:
         fc:e2:95:a2:b7:bd:57:d0:a3:68:b2:c1:2e:43:44:25:29:86:
         7c:d0:d0:87:93:fa:78:e8:af:59:d7:d7:e2:19:33:28:33:b9:
         8f:cc:c7:2b:60:a6:9c:e3:3f:e9:c6:06:58:e0:f5:08:a7:bc:
         88:81:5b:87
-----BEGIN CERTIFICATE-----
MIIDlzCCAn+gAwIBAgIJAM+PEWMj1Cj2MA0GCSqGSIb3DQEBCwUAMGIxGDAWBgNV
BAMMD2NsaWVudC5hbGUuY29tIDENMAsGA1UECgwEYWxlIDENMAsGA1UECwwEZXNk
IDEMMAoGA1UEBwwDYm4gMQ0wCwYDVQQIDARrYXIgMQswCQYDVQQGEwJpbjAeFw0x
NDAxMDMyMzA5MDdaFw0yNDAxMDEyMzA5MDdaMGIxGDAWBgNVBAMMD2NsaWVudC5h
bGUuY29tIDENMAsGA1UECgwEYWxlIDENMAsGA1UECwwEZXNkIDEMMAoGA1UEBwwD
Ym4gMQ0wCwYDVQQIDARrYXIgMQswCQYDVQQGEwJpbjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMxyehLTZhaPnyJZ0XoFAx+/UZMhjZV0GIh4cWIfCQQs
ztwKL7aIdsqdGvRziFSW6ISVgTyBdcRH20Snqhp1XT2wgqV8uF5d81CBG2KhBCtV
xC6bikjgOuC+VaM7VspcERR3NlQ1QU5A5ouMUC9lrdoE+TaNimhfuqBxMnv7uJU7
0Lus0L3bcCkIADqWXgzwD0UNNXhgBQ2y0BQdCCo5E+tuWDsJi65HGD4iJS4qkaaE
IYXkBYiLv2tvpQw/F5SgP1bX9pW2M85bezlXHWLg54w+T2SsGWgUw6/u8vpucMEj
EAxyraiHlKiZUtu2E7TsXmS5iRqKzsPb215pwE5DIlsCAwEAAaNQME4wHQYDVR0O
BBYEFGQJGWL4FP7tpbefxrqPsDA8sn+WMB8GA1UdIwQYMBaAFGQJGWL4FP7tpbef
xrqPsDA8sn+WMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAEjYrYYG
YckgZ9CzsmeHuQFJj4ub31v9snwfONHocxMpGmh6rthWc+hIBthqf0YrCPz0+yFg
9rnJE5NxG3+cGLDOPxKx5rmPzp9Oh4Mh4r4Kib4ZsxYU48C0lOcSwP7I/izwDHJc
bI8XtQ0l5H4SHjjXX3sNsqq712YzP0nu7xTAwth0PBo19DpTKhyIa+kgy3KyGoMM
k989dcTLyKtXGtwTvKnVjWQsu1Y6VMTkw3eFPf8h9dhINeDlB9f9BHz+0rg83Tjm
V/zilaK3vVfQo2iywS5DRCUphnzQ0IeT+njor1nX1+IZMygzuY/MxytgppzjP+nG
Bljg9QinvIiBW4c=
-----END CERTIFICATE-----
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa certificate generate-self-signed	Generates the X.509 self-signed certificate for TLS client authentication.
aaa certificate delete	Deletes the X.509 certificate.

MIB Objects

N/A

aaa certificate verify ca-certificate

Verifies the contents of the X.509 certificate.

aaa certificate verify ca-certificate *cert_file* **certificate** *cert_file*

Syntax Definitions

ca_cert_file	The X.509 certificate file (in PEM format) to be displayed.
cert_file	The X.509 certificate file (in PEM format) to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> aaa certificate verify ca-certificate ca_cert certificate cert_file
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa certificate generate-self-signed	Generates the X.509 self-signed certificate for TLS client authentication.
aaa certificate delete	Deletes the X.509 certificate.

MIB Objects

N/A

aaa certificate delete

Deletes the X.509 certificate.

aaa certificate delete *cert_file*

Syntax Definitions

cert_file	The X.509 certificate file (in PEM format) to be deleted.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> aaa certificate delete clientcert.pem
```

Release History

Release 8.3.1; command introduced.

Related Commands

aaa certificate generate-self-signed	Generates the X.509 self-signed certificate for TLS client authentication.
aaa certificate view	Displays the contents of the X.509 certificate.

MIB Objects

N/A

aaa certificate generate-csr

Generates the CSR (Certificate Signing Request) to be sent to get a CA signed certificate for TLS client authentication.

aaa certificate generate-csr {*csr_file***} key {***key_file***} [dn** *domain_name***} {CN** *common_name***} {ON** *org_name***} {OU** *org_unit***} {L** *locality***} {ST** *state***} {C** *country***}**

Syntax Definitions

csr_file	The name of the CSR certificate file to be created.
key_file	The name of the key file under which the RSA 2048 bit key is stored.
domain_name	Domain name to be used in the CSR.
common_name	Common Name used in X.509 certificate.
org_name	The Organization Name used in X.509 certificate.
org_unit	The Organization Unit used in X.509 certificate.
locality	The Locality used in X.509 certificate.
state	The State used in X.509 certificate.
country	The Country used in X.509 certificate.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Generates <csr_file>.pem file in **/flash/switch** directory. The <csr_file>.pem file created should be sent to CA signing authority to get the CA certificate.
- Default values will be taken for all other optional parameters while generating the CSR.
- The CSR needs to be created, sent to CA authority and the corresponding CA certificate (obtained from CA authority) should be uploaded to the **/flash/switch** directory before corresponding server configurations are done on the switch. If the CA certificate is uploaded post server configuration, then a switch reboot needs to be done for the changes to take effect.

Examples

```
-> aaa certificate generate-csr myCliCert.pem key clientkey.key days 3650 cn
client.ale.com on ALE ou ESD l BAN st KAR c IN
```

Release History

Release 8.3.1; command introduced.

Related Commands

show aaa common-criteria config	Displays the common criteria status on the switch.

MIB Objects

N/A

ssl pki client validate-certificate admin-state

Enables or disables the server's certification validation when the application on the switch acts as TLS client.

ssl pki client validate-certificate admin-state {enable | disable}

Syntax Definitions

enable	Enables the server's certification validation for the client application on the switch.
disable	Disables the server's certification validation for the client application on the switch.

Defaults

By default, the feature is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the feature is enabled or disabled, the switch must be rebooted for the changes to be applied.
- When the feature is enabled, TLS client (LDAP, RADIIUS, and SYSLOG) applications validate server certificate based on:
  - TLS mutual authentication using X.509 certificates.
  - The presented identifier must match the reference identifier as per RFC 6125 Section 6.
  - X.509 certificate validation using OCSP and CRL.

Examples

```
-> ssl pki client validate-certificate admin-state enable
-> ssl pki client validate-certificate admin-state disable
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ssl pki config	Displays the Public Key Infrastructure (PKI) configuration.

MIB Objects

```
systemSslPki
   systemSslPkiClientCertificateValidation
```

ssl pki client mutual-authentication admin-state

Enables or disables the mutual authentication for the TLS client applications on the switch.

ssl pki client mutual-authentication admin-state {enable | disable}

Syntax Definitions

enable	Enables the mutual authentication for the TLS client applications on the switch. When mutual-authentication is enabled, TLS client applications will need to load **myCliCert.pem**, **myCliPrivate.key** files in **/flash/switch/cert.d** and provide the certificate to server.
disable	Disables the mutual authentication for the TLS client applications on the switch.

Defaults

By default, the feature is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the feature is enabled or disabled, the switch must be rebooted for the changes to be applied.
- Enable this feature when the TLS client (LDAP, RADIUS, SYSLOG) applications needs to load the certificate **myCliCert.pem** and **myCliPrivate.key** file in **/flash/switch/cert.d/** directory and provide the certificate file to server while establishing TLS connection.
- If the server certificate doest not meet the validation criteria, the TLS client application connection is terminated.

Examples

```
-> ssl pki client mutual-authentication admin-state enable
-> ssl pki client mutual-authentication admin-state disable
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ssl pki config	Displays the Public Key Infrastructure (PKI) configuration.
ssl pki server mutual-authentication admin-state	Enables or disables the mutual authentication for the TLS server applications on the switch.
aaa certificate update-ca-certificate	Updates the CA-bundle with the custom CA server certificate provided by CA.

MIB Objects

```
systemSslPki
   systemSslPkiClientMutualAuthentication
```

ssl pki server mutual-authentication admin-state

Enables or disables the mutual authentication for the TLS server applications on the switch.

ssl pki server mutual-authentication admin-state {enable | disable}

Syntax Definitions

enable	Enables the mutual authentication for the TLS server applications on the switch. When mutual-authentication is enabled, the TLS server (SNMP) application will require clients to provide their certificate to server while establishing TLS connection.
disable	Disables the mutual authentication for the TLS server applications on the switch.

Defaults

By default, the feature is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the feature is enabled or disabled, the switch must be rebooted for the changes to be applied.
- Enable this feature when the TLS server (SNMP) application must require clients to provide their certificate to server while establishing TLS connection.
- When the feature is enabled, TLS server (SNMP) application validates client certificate based on:
  - TLS mutual authentication using X.509 certificates.
  - The presented identifier must match the reference identifier as per RFC 6125 Section 6.
  - X.509 certificate validation using OCSP and CRL.
- If the client certificate doest not meet the validation criteria, the TLS server application connection is terminated.

Examples

```
-> ssl pki server mutual-authentication admin-state enable
-> ssl pki server mutual-authentication admin-state disable
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ssl pki config	Displays the Public Key Infrastructure (PKI) configuration.
ssl pki client mutual-authentication admin-state	Enables or disables the mutual authentication for the TLS client applications on the switch.

MIB Objects

```
systemSslPki
   systemSslPkiServerMutualAuthentication
```

ssl pki tls version

Configures the TLS version for both TLS client and server applications.

ssl pki tls version {1.0 | 1.1 | 1.2}

Syntax Definitions

1.0	Sets the TLS version for client and server to 1.0.
1.1	Sets the TLS version for client and server to 1.1.
1.2	Sets the TLS version for client and server to 1.2.

Defaults

By default, the SSL PKI TLS version is 1.0.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The switch must be rebooted for the changes to be applied.
- When the TLS version is configured, TLS client and server applications will deny all SSL and TLS versions which are lower than the configured version.
- The command is applicable only for LDAP, RADIUS, SYSLOG and SNMP applications.

Examples

```
-> ssl pki tls version 1.0
-> ssl pki tls version 1.2
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ssl pki config	Displays the Public Key Infrastructure (PKI) configuration.

MIB Objects

```
systemSslPki
   systemSslPkiTlsVersion
```

show ssl pki config

Displays the Public Key Infrastructure (PKI) configuration.

show ssl pki config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ssl pki config
  SSL PKI Global Configuration:
  Client Validate Certificate = enabled
  Client Mutual Authentication = enabled
  Server Mutual Authentication = enabled
  TLS version = 1.2
```

Release History

Release 8.6R1; command introduced.

Related Commands

ssl pki client validate-certificate admin-state	Enables or disables the server's certification validation when the application on the switch acts as client.
ssl pki client mutual-authentication admin-state	Enables or disables the mutual authentication for the TLS client applications on the switch.
ssl pki server mutual-authentication admin-state	Enables or disables the mutual authentication for the TLS server applications on the switch.
ssl pki tls version	Configures the TLS version for both TLS client and server applications.

MIB Objects

```
systemSslPki
   systemSslPkiClientCertificateValidation
   systemSslPkiClientMutualAuthentication
   systemSslPkiServerMutualAuthentication
   systemSslPkiTlsVersion
```

ssl cipher

Selects the cipher security level for the applications using the OpenSSL.

ssl cipher {[level {all | high | medium | low}] | [custom {*string* | **file** *string***}]}**

Syntax Definitions

all	Includes all the cipher suites, including NULL-SHA.
high	Includes only AES-256 with SHA-2 ciphers (Applicable only for TLSv1.2).
medium	Includes all ciphers suites, except NULL-SHA, DES-CBC-SHA, and RC4-MD5.
low	Includes all cipher suites, except NULL-SHA.
string	Name of the cipher suite. It can be list of ciphers or a collective cipher file name. The custom cipher can have a maximum length of 255 characters in CLI and the cipher file can be of maximum 1024 bytes in size.

Defaults

By default, the SSL cipher security level is set to medium in default switch operation mode and high in common criteria mode.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To apply the new SSL cipher security level, switch must be rebooted.
- The command is applicable only for LDAP, Syslog, RADIUS, SNMP, and Captive Portal applications.
- Custom ciphers cannot be more than 255 characters. Hence, the cipher files can be used to configure ciphers more than 255 characters.
- The cipher file can be created by copying the required ciphers in the notepad and saving it as a cipher file with "**.cipher**" as the file extension.
- The ciphers for the custom cipher and cipher file must be from the supported list of ciphers. To view the supported ciphers, use the **show ssl ciphers all** command.
- The cipher file must be copied to the flash directory of the switch before using this command.
- In chassis based model, the cipher file needs to be copied in both the primary and secondary unit flash directory. In VC based models, the cipher file must be copied to all the flash directory of all the modules.

Examples

```
-> ssl cipher level all
-> ssl cipher level low
-> ssl cipher level medium
-> ssl cipher level high
```

```
-> ssl cipher custom AECDH-AES256-SHA
-> ssl cipher custom file /flash/abc.cipher
```

Release History

Release 8.6R1; command introduced.

Related Commands

show ssl ciphers all	Displays all the supported OpenSSL ciphers.
show ssl ciphers config	Displays the current cipher security level configuration.

MIB Objects

```
SSLCipherSuiteTable
   systemSslCipherLevel
   systemSslCipherSuite
```

show ssl ciphers all

Displays all the supported OpenSSL ciphers.

show ssl ciphers all

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The custom cipher suite must be configured based on the supported ciphers displayed in this output.

Examples

```
-> show ssl ciphers all
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:SRP-
DSS-AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-256-CBC-SHA:DH-DSS-AES256-GCM-
SHA384:DHE-DSS-AES256-GCM-SHA384:DH-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-
SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:DH-RSA-AES256-SHA256:DH-DSS-
AES256-SHA256:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DH-RSA-AES256-SHA:DH-DSS-
AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:DH-RSA-CAMELLIA256-
SHA:DH-DSS-CAMELLIA256-SHA:AECDH-AES256-SHA:ADH-AES256-GCM-SHA384:ADH-AES256-
SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-
AES256-GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-
SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:CAMELLIA256-
SHA:PSK-AES256-CBC-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
SHA:ECDHE-ECDSA-AES128-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-
128-CBC-SHA:DH-DSS-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:DH-RSA-AES128-GCM-
SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA256:DH-
RSA-AES128-SHA256:DH-DSS-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DH-
RSA-AES128-SHA:DH-DSS-AES128-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:DH-RSA-SEED-
SHA:DH-DSS-SEED-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:DH-RSA-
CAMELLIA128-SHA:DH-DSS-CAMELLIA128-SHA:AECDH-AES128-SHA:ADH-AES128-GCM-SHA256:ADH-
AES128-SHA256:ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ECDH-RSA-AES128-GCM-
SHA256:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES128-
SHA256:ECDH-RSA-AES128-SHA:ECDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-
SHA256:AES128-SHA:SEED-SHA:CAMELLIA128-SHA:IDEA-CBC-SHA:PSK-AES128-CBC-SHA:ECDHE-
RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:AECDH-RC4-SHA:ADH-RC4-MD5:ECDH-RSA-RC4-SHA:ECDH-
ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:ECDHE-RSA-DES-CBC3-SHA:ECDHE-ECDSA-DES-
CBC3-SHA:SRP-DSS-3DES-EDE-CBC-SHA:SRP-RSA-3DES-EDE-CBC-SHA:SRP-3DES-EDE-CBC-
SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DH-RSA-DES-CBC3-SHA:DH-DSS-DES-CBC3-
SHA:AECDH-DES-CBC3-SHA:ADH-DES-CBC3-SHA:ECDH-RSA-DES-CBC3-SHA:ECDH-ECDSA-DES-CBC3-
```

```
SHA:DES-CBC3-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-
SHA:AECDH-NULL-SHA:ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA:NULL-
MD5
```

Release History

Release 8.6R1; command introduced.

Related Commands

ssl pki client validate-certificate admin-state	Allows to select the cipher security level for the applications using the OpenSSL.
show ssl ciphers config	Displays the current cipher security level configuration.

MIB Objects

```
SSLCipherSuiteTable
   systemSslCipherSuite
```

show ssl ciphers config

Displays the current cipher security level configuration.

show ssl ciphers config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ssl ciphers config
  SSL Cipher Global Configuration:
  SSL Cipher Level = medium
  SSL Cipher Suite = ALL:eNULL:!NULL-SHA:!DES-CBC-SHA:!RC4-MD5

-> show ssl ciphers config
  SSL Cipher Global Configuration:
  SSL Cipher Level = custom-file
  SSL Cipher Suite File = /flash/abc.cipher
```

Release History

Release 8.6R1; command introduced.

Related Commands

ssl pki client validate-certificate admin-state	Allows to select the cipher security level for the applications using the OpenSSL.
show ssl ciphers all	Displays all the supported OpenSSL ciphers.

MIB Objects

```
SSLCipherSuiteTable
   systemSslCipherSuite
```

kerberos inactivity-timer

Configures global inactivity timer on the switch for Kerberos users.

kerberos inactivity-timer *num*

Syntax Definitions

num	Time interval in minutes.

Defaults

By default, inactivity timer is set to 300 minutes.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The valid range of inactivity timer is 10–600 minutes.
- Whenever a Kerberos user becomes inactive, then the inactivity timer will be started for that user. If Kerberos user becomes active before inactivity timer expiry, then timer will be stopped. User entry will be removed from the Kerberos user database on timer expiry.

Examples

```
-> kerberos inactivity-timer 30
```

Release History

Release 8.6R2; command introduced.

Related Commands

kerberos server-timeout	Configures global server reply time-out timer value on the switch for Kerberos users.
show kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaDaKerberosGlobalConfig
   alaDaKerberosGlobalInactivityTimer
```

kerberos ip-address

Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.

kerberos ip-address *ip_address* **[port** *num***]**

no kerberos ip-address *ip_address*

Syntax Definitions

ip_address	The IP address of the Kerberos server. (KDC)
num	UDP or TCP port number of the Kerberos application running on the Kerberos server. UDP port range is 1–65535.

Defaults

Default value of the port is 88.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- At least one Kerberos server and one Kerberos enabled port must be configured on the switch for Kerberos snooping to function.
- A maximum of two Kerberos server IP addresses can be configured on a switch
- Server IP address cannot be configured as 0.0.0.0, and the octet value in the IP address cannot be greater than 255 (for example, 1.256.2.3).
- Use the **port** keyword to configure both UDP and TCP protocol port number.
- Use the **no** form of this command to delete the Kerberos server IP address. Only one server can be deleted at a time.
- The UDP/TCP port number is not required to remove the Kerberos server IP address configuration.
- If all the authentication servers are removed from the switch, then all the Kerberos users learned so far on all the ports are not removed from the database.

Examples

```
-> kerberos ip-address 172.21.160.102 port 2001
-> kerberos ip-address 172.21.160.103 port 2003
-> no kerberos ip-address 172.21.160.102
```

Release History

Release 8.6R2; command introduced.

Related Commands

kerberos inactivity-timer	Configures a global inactivity timer on the switch for Kerberos users.
kerberos server-timeout	Configures a global server reply time-out timer value on the switch for Kerberos users.
show kerberos configuration	Displays the Kerberos global configuration.

MIB Objects

```
alaDaKerberosServerTable
   alaKerberosIpAddress
   alaDaKerberosUdpPort
   alaDaKerberosRowStatus
```

kerberos server-timeout

Configures global server reply time-out timer value on the switch for Kerberos users.

kerberos server-timeout *num*

Syntax Definitions

secs	Server reply time-out time interval in seconds in the range 1 second to 30 seconds.

Defaults

By default, reply-timeout is 2 seconds.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- All the users trying to get authenticated from a specific server will have the same value for reply-timeout timer.
- Whenever a Kerberos request packet is sent to the server, the server reply time-out starts. If the timer expires before receiving the reply from the server, the user authentication is marked as server-time-out and a trap is generated.

Examples

```
-> kerberos server-timeout 20
```

Release History

Release 8.6R2; command introduced.

Related Commands

show kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaDaKerberosGlobalConfig
   alaDaKerberosGlobalServerTimeoutTimer
```

kerberos authentication-pass policy-list-name

Configures a global classification QoS policy list on the switch for Kerberos users.

kerberos authentication-pass policy-list-name *policy_list*

no kerberos authentication-pass policy-list-name

Syntax Definitions

policy_list	Name of the QoS policy list.

Defaults

By default, there is no Kerberos global QoS policy list configured.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The QoS policy list must be created prior to this configuration.
- Per-user Kerberos policy list configuration is not supported.
- Use the **no** form of this command to remove the global classification QoS policy list from the switch.
- There is no validation done for QoS policy list in Kerberos. It is the user's responsibility to associate the correct QoS policy list with Kerberos.
- If the QoS policy list is deleted from the system, then the corresponding configuration in Kerberos will be removed and no error message will be thrown.
- If a domain level policy list is configured in the switch and any user belonging to that domain gets authenticated from the Kerberos server, then the domain level policy list is applied to the user over the global policy list.
- If a user gets authenticated from the Kerberos server and the domain level policy list is not configured on the switch for the authenticated user, then the global policy list is applied to the user if the global policy list is configured on the switch.
- If a user gets authenticated from the Kerberos server and neither the domain level policy list (for that user domain) nor the global policy list is configured, then the user traffic is classified on the basis of already applied non-supplicant authentication classification.

Examples

```
-> kerberos authentication-pass policy-list-name p2
```

The following example shows that the **p2** is configured as the global classification QoS policy list on the switch for Kerberos users.

```
-> show kerberos configuration
Inactivity Timer            :30 (mins),
Server Timeout              :20 (secs),
Global QoS Policy List      :p2,

Servers                     :
IP-Address           UDP Port
-----------------+---------------
1.1.1.1              88

Per Domain QoS policy List  :
Domain-Name                               Policy-List-Name
--------------------------------+-------------------------+--
EXAMPLE.COM                          p11
```

When the QoS policy list **p2** is removed from the system, the corresponding configuration in Kerberos is shown as below.

```
-> no policy list p2
-> qos apply

-> show kerberos configuration
Inactivity Timer            :30 (mins),
Server Timeout              :20 (secs),

Servers                     :
IP-Address           UDP Port
-----------------+---------------
1.1.1.1              88

Per Domain QoS policy List  :
Domain-Name                               Policy-List-Name         Status
--------------------------------+-----------------------------+----------
EXAMPLE.COM                          pl1                           active
```

The following command removes the global classification QoS policy list from the switch:

```
-> no kerberos authentication-pass policy-list-name
```

Release History

Release 8.6R2; command introduced.

Related Commands

kerberos ip-address	Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.
kerberos authentication-pass domain	Configures "per domain" classification policy for the Kerberos users.
show kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaDaKerberosGlobalConfig
   alaDaKerberosGlobalPolicy
```

kerberos authentication-pass domain

Configures a per-domain classification policy for the Kerberos users.

kerberos authentication-pass domain *domain_name* **policy-list-name** *policy_list*

no kerberos authentication-pass domain *domain_name*

Syntax Definitions

domain_name	Domain name on which the QoS policy is applied. Domain name length can be a maximum of 32 characters. Domain name is case sensitive.
policy_list	Name of the QoS policy list already configured.

Defaults

By default, there is no Kerberos global QoS policy list configured.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the per-domain classification policy for Kerberos users.
- Domain name is case sensitive.

Examples

```
-> kerberos authentication-pass domain EXAMPLE.COM policy-list-name p11
```

The following example shows that the **p11** is configured as the policy list associated with the domain EXAMPLE.COM:

```
-> show kerberos configuration
Inactivity Timer            :30 (mins),
Server Timeout              :20 (secs),

Servers                     :
IP-Address           UDP Port
-----------------+----------------
1.1.1.1              88

Per Domain QoS policy List  :
Domain-Name                               Policy-List-Name
--------------------------------+--------------------------
EXAMPLE.COM                          pl1
```

When the QoS policy list **p11** is removed from the system, the corresponding configuration in Kerberos is shown as below.

```
-> no policy list pl1
-> qos apply
```

```
-> show kerberos configuration
Inactivity Timer            :30 (mins),
Server Timeout              :20 (secs),

Servers                     :
IP-Address           UDP Port
-----------------+---------------
1.1.1.1              88

Per Domain QoS policy List  :
Domain-Name                              Policy-List-Name
---------------------------------+-----------------------------+
EXAMPLE.COM                          pl1
```

The following command removes the per-domain classification policy for Kerberos users:

```
-> no kerberos authentication-pass domain EXAMPLE.COM
```

Release History

Release 8.6R2; command introduced.

Related Commands

kerberos authentication-pass policy-list-name	Configures global classification QoS policy list on the switch for Kerberos users.
show kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaDaKerberosPolicyConfigTable
  alaDaKerberosPolicyName
  alaDaKerberosPolicyRowStatus
```

clear kerberos statistics

Clears Kerberos statistics.

clear kerberos statistics

Syntax Definitions

N/A

Defaults

By default, global statistics are cleared.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to clear global Kerberos statistics.

Examples

```
-> clear kerberos statistics
```

Release History

Release 8.6R2; command introduced.

Related Commands

show kerberos configuration	Displays Kerberos global configuration.

MIB Objects

```
alaKerberosGlobalClearStats
```

show kerberos configuration

Displays Kerberos global configuration.

show kerberos configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display information about Kerberos settings configured through the **kerberos inactivity-timer** command.

Examples

```
-> show kerberos configuration

Inactivity Timer            :30 (mins),
Server Timeout              :9 (secs),
Global QoS Policy List      :p2,

Servers                     :
IP-Address            UDP Port
------------------+----------------
1.2.3.5               90
4.5.6.7               88
11.22.33.55           80

Per Domain QoS policy List  :
Domain-Name                        Policy-List-Name                 Status
-------------------------------+-------------------------------+----------------
EXAMPLE.COM                          pl1                           Active
```

output definitions

Inactivity Timer	Global inactivity timer configured on the switch for Kerberos users.
Server Timeout	Global server reply time-out timer value configured on the switch for Kerberos users.
Global QoS Policy List	Global classification QoS policy list associated with the Kerberos users
Servers	**IP Address**: IP address configured of the Kerberos server. **UDP Port**: UDP or TCP port of the Kerberos application running on the Kerberos server.

output definitions (continued)

Per Domain QoS policy List	**Domain-Name**: Per-domain classification policy configured for Kerberos users. **Policy-List-Name**: Name of the QoS policy list associated with the domain. **Status**: Per-domain QoS policy list status (**Active** or **Inactive**). Inactive status indicates that the policy list does not exist in the switch or the policy list exists, but is not applied.

Release History

Release 8.6R2; command introduced.

Related Commands

kerberos inactivity-timer	Configures global inactivity timer on the switch for Kerberos users.
kerberos ip-address	Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.
kerberos server-timeout	Configures global server reply time-out timer value on the switch for Kerberos users.
kerberos authentication-pass policy-list-name	Configures global classification QoS policy list on the switch for Kerberos users.
kerberos authentication-pass domain	Configures per-domain classification policy for the Kerberos users.
show kerberos users	Displays the learned Kerberos users information.
show kerberos statistics	Displays the global Kerberos statistics.
clear kerberos statistics	Clears global Kerberos statistics.

MIB Objects

```
alaDKerberosGlobalConfig
   alaKerberosGlobalInactivityTimer
   alaKerberosGlobalServerTimeoutTimer
   alaKerberosGlobalPolicy
alaKerberosServerTable
   alaKerberosIpAddress
   alaKerberosUdpPort
alaKerberosPolicyConfigTable
   alaKerberosPolicyDomainName
   alaKerberosPolicyName
```

show kerberos users

Displays the learned Kerberos users information.

show kerberos users [port *chassis/slot/port* **|linkagg** *agg_id* **| mac-address** *mac_address* | **count]**

Syntax Definitions

chassis	The Chassis Identifier.
slot/port	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
agg_id	Enter a link aggregate ID number.
mac_address	MAC address of the Kerberos user.
count	Displays the number of Kerberos users.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a *chassis/slot/port* is specified, the Kerberos users learned on that port are displayed.
- If *agg_id* is specified, the Kerberos users learned on that link aggregate are displayed.
- If a MAC address is specified, then the information related to that Kerberos user is displayed.
- If none of the parameters are specified (chassis/slot/port, MAC address), then the information related to all the Kerberos users learned on the switch is displayed.

Examples

```
-> show kerberos users
 Port    Username          MAC Address       Auth Status      QOS Policy Domain
-------+-----------------+-----------------+-----------------+----------+----------
2/1/18  root/admin        00:11:22:33:44:55 tgs-authenticated    pl1     AP01.ORG
2/1/19  guest             00:01:02:03:04:05 tgs-timeOut                  AP01.ORG

-> show kerberos users port 2/1/18
 Port    Username          MAC Address       Auth Status      QOS Policy Domain
-------+-----------------+-----------------+-----------------+----------+---------
2/1/18  root/admin         00:11:22:33:44:55  tgs-authenticated    pl1    AP01.ORG
```

output definitions

Port	The Kerberos chassis, slot, and port number.
Username	User name of the client.

output definitions (continued)

MAC Address	MAC address of the Kerberos user.
Auth Status	Kerberos authentication process involves exchange of two requests (AS_REQ and AS_REP) and two response (AS_REP and TGS_REP). This field indicates up to which level the authentication has reached. On successful authentication, "tgs-authenticated" is displayed.
QoS Policy	QoS policy list configured on the switch for the Kerberos user.
Domain	Per-domain classification policy configured for the Kerberos user.

```
-> show kerberos users mac-address 00:11:22:33:44:55
Detail User Information:
  MAC Address            : 00:11:22:33:44:55
  Port                   : 1/1/1
  Authentication Status  : tgs-authenticated
  QoS Policy             : pl1
  Domain Name            : EXAMPLE.COM
  User Name              : root\admin
  User Entry State       : active
  Inactivity Timer Left  : NA
```

output definitions

MAC Address	MAC address of the Kerberos user.
Port	The Kerberos chassis, slot, and port number.
Authentication Status	Kerberos authentication process involves exchange of two requests (AS_REQ and AS_REP) and two response (AS_REP and TGS_REP). This field indicates up to which level the authentication has reached. On successful authentication, "tgs-authenticated" is displayed.
QoS Policy	QoS policy list configured on the switch for the Kerberos user.
Domain Name	Per-domain classification policy configured for the Kerberos user.
User Name	User name of the client.
User Entry State	The current state of the user.
Inactivity Timer Left	The amount of time left, in seconds, of the inactivity timer value.

Release History

Release 8.6R2; command introduced.

Related Commands

kerberos authentication-pass policy-list-name	Configures global classification QoS policy list on the switch for Kerberos users.
kerberos authentication-pass domain	Configures per-domain classification policy for the Kerberos users.
show kerberos configuration	Displays Kerberos global configuration.
clear kerberos statistics	Clears global Kerberos statistics.

MIB Objects

```
alaDaKerberosUserTable
   alaDaKerberosUserMac
   alaDaKerberosUserPort
   alaDaKerberosUserName
   alaDaKerberosUserDomain
   alaDaKerberosUserAuthState
   alaDaKerberosUserPolicy
   alaDaKerberosUserLeftTime
   alaDaKerberosUserState
```

show kerberos statistics

Displays global Kerberos statistics.

show kerberos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display the global Kerberos statistics.

Examples

```
-> show kerberos statistics
Total Client Packet Rx         :  52
Total Server Packet Rx         :  13
Total KRB-AS-REQ Packet Rx     :  47
Total KRB-AS-REP Packet Rx     :  8
Total KRB-TGS-REQ Packet Rx    :  5
Total KRB-TGS-REP Packet Rx    :  5
Total KRB-ERROR Packet Rx      :  0
Total Client Packet Sw Discard :  0
Total Server Packet Sw Discard :  2
```

output definitions

Total Client Packet Rx	Total client request packets received.
Total Server Packet Rx	Total server response packets received.
Total KRB-AS-REQ Packet Rx	Total AS-REQ request packets received.
Total KRB-AS-REP Packet Rx	Total AS-REP response packets received.
Total KRB-TGS-REQ Packet Rx	Total TGS-REQ request packets received.
Total KRB-TGS-REP Packet Rx	Total TGS-REP response packets received.
Total KRB-ERROR Packet Rx	Total error packets received from the server.
Total Client Packet Sw Discard	Total client's request packets discarded at software by Kerberos module.
Total Server Packet Sw Discard	Total server's response packets discarded at software by Kerberos module.

Release History

Release 8.6R2; command introduced.

Related Commands

show kerberos configuration	Displays Kerberos global configuration.
clear kerberos statistics	Clears global and port-level Kerberos statistics.

MIB Objects

```
alaDaKerberosTotalClientPktRxStats
alaDaKerberosTotalServerPktRxStats
alaDaKerberosClientPktSwDiscardStats
alaDaKerberosServerPktSwDiscardStats
alaDaKerberosTotalASREQRxStats
alaDaKerberosTotalASREPRxStats
alaDaKerberosTotalTGSREQRxStats
alaDaKerberosTotalTGSREPRxStats
alaDaKerberosTotalErrorRxStats
```

aaa jitc admin-state

Enables or disables Joint Interoperability Test Command (JITC) mode on the switch.

aaa jitc admin-state {enable | disable}

Syntax Definitions

enable | disable	Enables or disables the JITC (Joint Interoperability Test Command) mode.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configuration is applied only after a reload of the switch.
- The JITC mode is mutually exclusive of Common Criteria mode and Enhanced-mode. If the switch is already running in Common Criteria or enhanced-mode (NIS) it must be disabled before enabling JITC mode and vise versa.

Examples

```
-> aaa jitc admin-state enable
WARNING: JITC mode configuration is applied only after reload
```

Release History

Release 8.4.1; command introduced.

Related Commands

show aaa jitc config	Displays the JITC status on the switch.

MIB Objects

N/A

show aaa jitc config

Displays the JITC status on the switch.

show aaa jitc config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show aaa jitc config
Admin State: Enabled,
Operational State: Enabled
```

output definitions

Admin State	Indicates configuration status of JITC mode (**Enabled** or **Disabled**).
Operational State	Indicates operational status of JITC mode (**Enabled** or **Disabled**).

Release History

Release 8.4.1; command introduced.

Related Commands

aaa jitc admin-state	Enables or disables JITC mode on the switch.

MIB Objects

N/A

39 Access Guardian Commands

Access Guardian refers to a set of OmniSwitch security functions that work together to provide a dynamic, proactive network security solution. This chapter provides information about the commands that are used to configure the following Access Guardian features through the Command Line Interface (CLI):

- **Universal Network Profile (UNP)**—Access Guardian is configured and applied through the framework of the UNP feature. UNP is enabled on switch ports to activate Access Guardian functionality that is used to authenticate and classify users into UNP profiles. Each profile is mapped to a VLAN ID or Service Access Point (SAP) to which the user is dynamically assigned. Specific UNP port configurations help to simplify and easily replicate the same configuration across multiple ports.
- **Bring Your Own Device (BYOD) - OmniSwitch / UPAM or ClearPass Integration**: The OmniSwitch leverages Access Guardian functionality along with the OmniVista Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) to provide an overall BYOD solution.
  - Configurable UNP port and profile attributes are used to redirect traffic from the OmniSwitch to the UPAM or CPPM server.
  - Configurable GRE tunnels allow the OmniSwitch to intercept and tunnel Multicast Domain Name System (mDNS) and Simple Service Discovery Protocol (SSDP) packets to or from a WLAN controller in a BYOD network.
- **Captive Portal**—Internal and external Captive Portal Web-based authentication. Internal Captive Portal authentication is provided through an internal Web server on the OmniSwitch that presents default or customized Web pages to the user. A post-authentication and/or post-classification process to validate user credentials and dynamically assign a new role (policy list) to enforce user access to the network. External, guest Captive Portal authentication is provided through the OmniSwitch Access Guardian interaction with the OmniVista Unified Policy Access Manager or the ClearPass Policy Manager.
- **Quarantine Manager and Remediation (QMR)**—QMR is a switch-based application that restricts the network access of known quarantined users and provides a remediation path to allow quarantined users to regain their network access.
- **IoT Device Profiling IoT**—Device Profiling allows the network administrators to support and manage smart phones, Tablets and other devices connecting to the network. The IoT Device Profiling uses DHCP FingerPrinting and MAC OUI (MAC Vendors) to identify IoT devices.

For commands used to configure device authentication, authorization, and accounting parameters that are used to support Access Guardian functionality, see “Chapter 38, “AAA Commands.”

For commands used to configure Learned Port Security (LPS), which is used by Access Guardian to help ensure that only certain devices are allowed to connect to the switch, see “Chapter 46, “Learned Port Security Commands.”

MIB information for the UNP commands is as follows:

Filename: ALCATEL-IND1-DA-MIB.mib
Module: alcatelIND1DaMIB

Filename: ALCATEL-IND1-UDP-RELAY-MIB.mib
Module: alcatelIND1UDPRelayMIB

A summary of the available commands is listed here:

UNP Global Configuration Commands	**unp dynamic-vlan-configuration** **unp dynamic-profile-configuration** **unp delay-learning** **unp auth-server-down** **unp auth-server-down-timeout** **unp policy validity-period** **unp policy validity-location** **unp domain description** **unp redirect port-bounce** **unp redirect pause-timer** **unp redirect proxy-server-port** **unp redirect-server** **unp redirect allowed-name** **unp force-l3-learning** **unp 802.1x-pass-through** **unp ipv6-drop** **unp ap-mode** **unp mac-mobility** **unp user flush** **show unp global configuration** **show unp domain** **show unp user** **show unp user status** **show unp user details** **show unp policy validity-period** **show unp policy validity-location**

UNP Profile Commands	**unp profile** **unp profile qos-policy-list** **unp profile location-policy** **unp profile period-policy** **unp profile captive-portal-authentication** **unp profile captive-portal-profile** **unp profile kerberos-authentication** **unp profile authentication-flag** **unp profile mobile-tag** **unp profile maximum-ingress-bandwidth** **unp profile maximum-egress-bandwidth** **unp profile maximum-ingress-depth** **unp profile maximum-egress-depth** **unp profile inactivity-interval** **unp profile mac-mobility** **unp profile saa-profile** **unp profile map vlan** **unp profile map service-type spb** **unp profile map service-type vxlan** **unp vxlan far-end-ip-list** **unp profile map service-type l2gre** **unp l2gre far-end-ip-list** **unp profile map service-type static** **show unp profile** **show unp profile map** **show unp vxlan far-end-ip-list** **show unp l2gre far-end-ip-list**
UNP System Default Profile Commands	**unp system-default service-mod** **unp system-default service-base** **unp system-default multicastmode** **unp system-default vlan-xlation** **unp system-default multicastgroup** **unp system-default far-end-ip-list** **show unp global configuration**
UNP SAA Profile Commands	**unp saa-profile** **show unp saa-profile**
Device Profiling Commands	**device-profile admin-state** **device-profile port linkagg** **device-profile device-type** **device-profile update-signature** **device-profile update-signature from** **device-profile auto-unp-assignment** **show device-profile config** **show device-profile summary** **show device-profile catalog** **show device-profile signatures from** **show device-profile signatures**

UNP Port Commands	**unp port-type** **unp l2-profile** **unp redirect port-bounce** **unp 802.1x-authentication** **unp 802.1x-authentication pass-alternate** **unp 802.1x-authentication tx-period** **unp 802.1x-authentication supp-timeout** **unp 802.1x-authentication max-req** **unp 802.1x-authentication bypass-8021x** **unp 802.1x-authentication failure-policy** **unp mac-authentication** **unp mac-authentication pass-alternate** **unp mac-authentication allow-eap** **unp classification** **unp trust-tag** **unp default-profile** **unp domain** **unp aaa-profile** **unp port port-template** **unp direction** **unp admin-state** **unp dynamic-service** **unp vlan** **unp port profile** **unp force-l3-learning** **unp port ap-mode** **show unp port** **show unp port config** **show unp port bandwidth** **show unp port 802.1x statistics** **show unp port configured-vlans** **show unp port profile**
UNP Port Template Commands	**unp port-template** **show unp port-template**
Router Domain Authentication	**unp network-group** **unp router-auth user-group** **unp router-auth cp-profile** **unp router-auth user flush** **show unp network-group** **show unp router-auth user-group** **show unp router-auth configuration** **show unp router-auth users**
Classification Rule Commands	**unp classification port** **unp classification domain** **unp classification mac-address** **unp classification mac-oui** **unp classification mac-range** **unp classification ip-address** **unp classification vlan-tag** **unp classification lldp med-endpoint** **unp classification authentication-type** **show unp classification**

Extended Classification Rule Commands	**unp classification-rule** **unp classification-rule port** **unp classification-rule domain** **unp classification-rule mac-address** **unp classification-rule mac-oui** **unp classification-rule mac-range** **unp classification-rule ip-address** **unp classification-rule vlan-tag** **unp classification-rule lldp med-endpoint** **unp classification-rule authentication-type** **unp classification-rule device-type** **show unp classification-rule**
User Role Commands	**unp user-role** **unp user-role policy-list** **unp user-role profile** **unp user-role authentication-type** **unp user-role cp-status-post-login** **unp restricted-role policy-list** **show unp user-role** **show unp restricted-role**
Captive Portal Commands	**captive-portal mode** **captive-portal name** **captive-portal ip-address** **captive-portal success-redirect-url** **captive-portal proxy-server-port** **captive-portal retry-count** **captive-portal authentication-pass** **captive-portal authentication-pass domain** **captive-portal-profile** **captive-portal customization** **show captive-portal configuration** **show captive-portal profile-names**
Quarantine Manager and Remediation (QMR) Commands	**qmr quarantine path** **qmr quarantine page** **qmr quarantine allowed-name** **qmr quarantine custom-proxy-port** **show qmr** **show quarantine mac group**

Zero Configuration Networking Commands (mDNS and SSDP)	**zeroconf mdns admin-state** **zeroconf ssdp admin-state** **zeroconf mode** **zeroconf responder-ip** **zeroconf gateway-vlan-list** **zeroconf access-vlan-list** **zeroconf server-policy** **zeroconf client-policy** **zeroconf service-rule policy** **zeroconf service-rule service-id** **zeroconf service-list** **zeroconf service-id query-request** **zeroconf edge-ip-list** **zeroconf refresh-database** **show zeroconf** **show zeroconf services** **show zeroconf services-cache** **show zeroconf edge-details** **show zeroconf server policies** **show zeroconf client policies** **show zeroconf service rules** **show zeroconf server policy-instances**

unp dynamic-vlan-configuration

Configures the UNP status for dynamic VLAN configuration. When this functionality is enabled and a VLAN mapping is configured with a VLAN ID that does not exist, the switch will dynamically create the necessary VLAN ID.

unp dynamic-vlan-configuration

no unp dynamic-vlan-configuration

Syntax Definitions

N/A

Defaults

By default, dynamic VLAN configuration is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Note. Dynamic VLANs are not saved in the VLAN section of the **boot.cfg** file. However, the **unp** commands to enable dynamic VLAN configuration and create a UNP are saved in the UNP section of the **boot.cfg** file. As a result, the VLAN is created again on the next switch bootup.

- Use the **no** form of this command to disable dynamic VLAN configuration.
- When dynamic VLAN configuration is disabled, configuring a VLAN mapping with a VLAN ID that does not exist in the switch configuration is not allowed.
- The VLAN status and other port (non-UNP port) assignments for a dynamic UNP VLAN are configurable using standard VLAN commands. In addition, the STP status is configurable and enabled by default when the dynamic VLAN is created.
- A dynamic VLAN cannot be deleted using standard VLAN commands (**no vlan** *vlan_id*).
- UNP dynamic VLANs are identified as a separate type of VLAN. The **show vlan** command will display this type with the default name of “UNP-DYN-VLAN” and the designated type as “UNP Dynamic Vlan”.

Examples

```
-> unp dynamic-vlan-configuration
-> no unp dynamic-vlan-configuration
```

Release History

Release 7.2.1; command was introduced.

Related Commands

unp profile	Configures a UNP in the switch configuration.
show unp global configuration	Displays the dynamic VLAN configuration status for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPDynamicVlanConfigFlag
```

unp dynamic-profile-configuration

Configures the UNP status for dynamic profile configuration. When this functionality is enabled, a UNP profile is dynamically created based on specific traffic conditions.

unp dynamic-profile-configuration

no unp dynamic-profile-configuration

Syntax Definitions

N/A

Defaults

By default, dynamic profile configuration is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable dynamic profile configuration.
- When dynamic profile configuration is enabled, a UNP profile is dynamically created when the trust VLAN tag option is enabled on the UNP port or link aggregate and one of the following conditions occurs:
  - A tagged packet received on the UNP port contains a VLAN tag that matches an existing MVRP VLAN in the switch configuration that is not assigned to a profile.
  - There is no matching VLAN in the switch configuration.
- Dynamically created profiles are saved in the **boot.cfg** file for the switch.
- By default, dynamically created profiles are automatically named **dynamic_profile_***vlan_id*, where the VLAN ID is the ID of the VLAN contained in the packet tag.
- After the dynamic profile is created, changing the profile name, the associated VLAN ID, or the QoS policy list is allowed. To avoid any confusion, change the profile name if the VLAN ID associated with the profile has changed.
- If the dynamic profile configuration option is enabled along with the dynamic VLAN configuration option and a dynamically created profile refers to a VLAN that is an MVRP VLAN, then the MVRP VLAN is automatically converted to a dynamic UNP VLAN (UNP-DYN-VLAN).

Examples

```
-> unp dynamic-profile-configuration
-> no unp dynamic-profile-configuration
```

Release History

Release 7.2.1.R02; command was introduced.

Related Commands

unp profile	Configures a UNP in the switch configuration.
unp dynamic-vlan-configuration	Configures the status of dynamic VLAN configuration. When enabled, UNP will create a VLAN at the time a VLAN mapping for a profile is created that specifies a VLAN ID that does not exist in the switch configuration.
show unp global configuration	Displays the dynamic profile configuration status for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPDynamicProfileConfigFlag
```

unp delay-learning

Configures the UNP delay learning time interval. This specifies the amount of time, in seconds, that UNP will delay learning packets received on UNP ports.

unp delay-learning *seconds*

Syntax Definitions

seconds	The amount of time to wait before UNP learning starts. The valid range is 0–600 seconds.

Defaults

By default, the delay learning timer is disabled (timer value is set to 0).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To disable the delay learning timer, set the timer value to zero (the default).
- The configured time interval is triggered when the switch boots up. During this time, any packets received on all UNP ports are dropped until the timer expires.
- Configuring a delay learning interval gives the switch time to bring up IP interfaces and for route convergence to complete before any attempt to reach an authentication server is made.

Examples

```
-> unp delay-learning 250
-> unp delay-learning 600
-> unp delay-learning 0
```

Release History

Release 8.5R2; command was introduced.

Related Commands

unp auth-server-down	Configures a UNP to which a device is classified if MAC or 802.1X authentication fails because the RADIUS server is not reachable.
show unp global configuration	Displays the UNP delay learning timer value for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPDelayLearning
```

unp auth-server-down

Configures a UNP profile to which a device is classified if authentication fails because the RADIUS server is unreachable.

unp auth-server-down {profile1 *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp auth-server-down [profile1] [profile2] [profile3]

Syntax Definitions

profile_name	The name of an existing profile to which the device is assigned when the authentication server is unreachable.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an authentication server down UNP profile.
- When a device is classified into the specified profile, a configurable authentication down timer is started for that device. When the timer runs out, the authentication process is performed again. If authentication fails again, the device is classified back into the authentication server down profile. The switch will repeat this process until the device authentication is completed.
- Configuring an authentication server down UNP is highly recommended when MAC or 802.1X authentication is enabled on any UNP port or link aggregate. This is because after a switch reload, the traffic from devices connected to UNP ports and link aggregates reaches the switch and triggers the authentication process before route convergence has completed and the server can be reached.
  - If an authentication server down UNP is configured, devices are temporarily learned in that profile and authentication is automatically attempted again after the timeout period expires. This allows time for the server to become reachable from the switch after a reload.
  - If an authentication server down UNP is not configured, devices are learned as filtering and will remain in that state. There is no further attempt to authenticate these devices again.
- If the authentication server down UNP is removed, the authentication server down timer is also removed.
- Up to three different profile names are configurable as authentication server down UNP profiles. The profile applied to the traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to device traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to device traffic received on UNP access ports.
  - When multiple profiles are configured, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the device traffic.

- Configuring both a VLAN profile and a service profile ensures that an authentication server down UNP is available for device traffic received on both types of UNP ports (bridge and access).

Examples

```
-> unp auth-server-down profile1 unp1-vlan
-> no unp auth-server-down profile1
-> unp auth-server-down profile1 unp1-vlan profile2 unp2-vxlan
-> no unp auth-server-down profile1 profile2
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.4; command syntax changed; **vxlan-profile** parameter added.
Release 8.3.1; **vlan-profile** and **vxlan-profile** parameters replaced with **profile1**, **profile2**, and **profile3** parameters.

Related Commands

unp auth-server-down-timeout	Configures the value for the authentication server down timer.
show unp global configuration	Displays the profiles designated as the authentication server down UNP for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPAuthServerDownUnp
```

unp auth-server-down-timeout

Configures the authentication server down timer value. This timer value is applied to devices that are learned in the authentication server down UNP.

unp auth-server-down-timeout *seconds*

no unp auth-server-down-timeout

Syntax Definitions

seconds	The number of seconds the authentication server down timer is active.The valid range is 10 to 1000 seconds.

Defaults

By default, the timeout value is set to 60 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to set the timer value back to the default value (60 seconds).
- When this timer expires, devices learned in the authentication server down UNP are cleared from that UNP. The authentication and classification process is attempted again.
- When the authentication server down UNP is removed, the authentication server down timer is also cleared.

Examples

```
-> unp auth-server-down-timeout 500
-> unp auth-server-down-timeout 120
-> no unp auth-server-down-timeout
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.4; command syntax changed; **vxlan-profile** parameter added.
Release 8.3.1; **vlan-profile** and **vxlan-profile** parameters deprecated.

Related Commands

unp auth-server-down	Configures a UNP to which a device is classified if MAC or 802.1X authentication fails because the RADIUS server is not reachable.
show unp global configuration	Displays the authentication server down timeout value for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPAuthServerDownTimeout
```

unp policy validity-period

Configures a UNP validity period policy that specifies the days and times during which a device can access the network. This type of policy is assigned to a UNP profile and applied to devices classified into the profile. A device must match all of the policy criteria.

unp policy validity-period *policy_name* **[days** *days***] [months** *months***] [hours** *hh:mm* **to** *hh:mm***] [interval** *mm:dd:yy hh:mm* **to** *mm:dd:yy hh:mm***] [timezone** *zones***]**

no unp policy validity-period *policy_name* **[days** *days* **| months** *months* **| hours** | **interval | timezone]**

Syntax Definitions

policy_name	The name of the validity period policy (up to 31 alphanumeric characters).
days	The day(s) of the week this validity period is active. Enter the actual day of the week (e.g., **monday**, **tuesday**, **wednesday**, etc.).
months	The month(s) in which the validity period is active. Enter the actual month (e.g., **january**, **february**, **march**, etc.).
hh:mm	The time of day, specified in hours and minutes, the validity period starts and the time of day the validity period ends (e.g., 10:30 to 11:30).
mm:dd:yy hh:mm	An interval of time during which the validity period is active. Specify a start and end to the interval period by entering a beginning date and time followed by an end date and time (e.g., 11:01:17 12:01 to 11:02:17 12:01).
zones	The timezone in which the validity period is active (for example, **pst**, **est**, **gmt**, etc.)

Defaults

parameter	default
days	no restriction
months	no restriction
hh:mm	no specific time
mm:dd:yyyy hh:mm	no interval
zones	local timezone

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a UNP period policy from the configuration, or to remove parameters from a particular validity period policy.

- Any combination of the **days**, **months**, **hours**, **interval**, and **timezone** parameters is allowed. The validity period is only in effect when all specified parameters are true.
- Use the **unp profile period-policy** command to associate a period policy with a UNP profile.

Examples

```
-> unp policy validity-period Office-Time
-> no unp policy validity-period Office-Time

-> unp policy validity-period Office-Time days monday
-> unp policy validity-period Office-Time days monday time-zone IST
-> no unp policy validity-period Office-Time time-zone
-> no unp policy validity-period Office-Time days monday

-> unp policy validity-period Office-Time days all
-> unp policy validity-period Office-Time days all time-zone PST
-> no unp policy validity-period Office-Time days saturday sunday

-> unp policy validity-period Office-Time hours 9:00 to 17:00
-> unp policy validity-period Office-Time hours 9:00 to 17:00 time-zone IST
-> no unp policy validity-period Office-Time hours

-> unp policy validity-period Holiday months december january
-> no unp policy validity-period Holiday months january

-> unp policy validity-period Holiday months december time-zone IST
-> no unp policy validity-period Holiday time-zone
-> no unp policy validity-period Holiday months december

-> unp policy validity-period Seminar interval 02/01/13 10:30 to 02/05/13 16:00
-> no unp policy validity-period Seminar interval

-> unp policy validity-period Seminar interval 02/01/13 10:30 to 02/05/13 16:00
time-zone PST
-> no unp policy validity-period Seminar time-zone
-> no unp policy validity-period Seminar interval
```

Release History

Release 8.1.1; command introduced.

Related Commands

unp profile period-policy	Assigns a UNP period policy to a profile.
show unp policy validity-period	Displays information about the UNP period policy configuration.

MIB Objects

```
alaDaUNPValidityPeriodTable
   alaDaUNPValidityPeriodName
   alaDaUNPValidityPeriodDays
   alaDaUNPValidityPeriodDaysStatus
   alaDaUNPValidityPeriodMonths
   alaDaUNPValidityPeriodMonthsStatus
   alaDaUNPValidityPeriodHour
   alaDaUNPValidityPeriodHourStatus
   alaDaUNPValidityPeriodEndHour
   alaDaUNPValidityPeriodInterval
   alaDaUNPValidityPeriodIntervalStatus
   alaDaUNPValidityPeriodEndInterval
   alaDaUNPValidityPeriodTimezone
   alaDaUNPValidityPeriodTimezoneStatus
   alaDaUNPValidityPeriodActiveStatus
```

unp policy validity-location

Configures a UNP validity location policy that defines a specific location from which a device can access the network. This type of policy is assigned to a UNP profile and applied to devices classified into the profile. A device must match all of the policy criteria defined.

unp policy validity-location *policy_name* **[port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]** **[system-name** *system_name***] [system-location** *system_location***]**

no unp policy validity-location *policy_name* **[port | linkagg | system-name | system-location]**

Syntax Definitions

policy_name	The name of the validity location policy (up to 31 alphanumeric characters).
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1) of a UNP port. Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number of a UNP link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).
system_name	The configured system name for the switch from which the device can access the network.
system_location	The configured system location for the switch from which the device can access the network.

Defaults

parameter	default
*chassis/slot/port***[**-*port2***]**	no restriction
*agg_id***[**-*agg_id2***]**	no restriction
system_name	no restriction
system_location	no restriction

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a UNP location policy from the configuration, or to remove parameters from a particular location policy.
- Any combination of the **port**, **linkagg**, **system-name**, and **system-location** parameters is allowed. The location policy is only in effect when all specified parameters are true.
- Use the **unp profile location-policy** command to associate a location policy with a UNP profile.

Examples

```
-> unp policy validity-location ALU-NA
-> no unp policy validity-location ALU-NA

-> unp policy validity-location ALU-NA port 1/1/10
-> unp policy validity-location ALU-NA port 1/1/1-5
-> no unp policy validity-location ALU-NA port

-> unp policy validity-location ALU-NA linkagg 10
-> unp policy validity-location ALU-NA linkagg 1-5
-> no unp policy validity-location ALU-NA linkagg

-> unp policy validity-location ALU-NA system-name OS6860
-> no unp policy validity-location ALU-NA system-name OS6860

-> unp policy validity-location ALU-NA system-location US-West
-> no unp policy validity-location ALU-NA system-location
```

Release History

Release 8.1.1; command introduced.

Related Commands

unp profile location-policy	Assigns a UNP location policy to a profile.
show unp policy validity-location	Displays information about the UNP location policy configuration.

MIB Objects

```
alaDaUNPLocationPolicyTable
   alaDaUNPLocationPolicyName
   alaDaUNPLocationPolicyPort
   alaDaUNPLocationPolicyPortHigh
   alaDaUNPLocationPolicyPortStatus
   alaDaUNPLocationPolicySystemName
   alaDaUNPLocationPolicySystemLocation
```

unp domain description

Configures a customer domain ID to which UNP ports and classification rules are assigned.

unp domain *domain_id* **[description** *domain_description***]**

no unp domain *domain_id* **description** *domain_description*

Syntax Definitions

domain_id	A numerical customer domain ID.
domain_description	An alphanumeric string (1–128 characters).

Defaults

By default, customer domain ID zero (0) is assigned to all UNP ports.

parameter	default
domain_description	Domain ID

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the customer domain ID from the switch configuration. When a domain ID is removed, the following actions are triggered:
  - All UNP ports assigned to that domain are moved to the default domain ID 0.
  - Any classification rules assigned to that domain are removed.
- Customer domains are used to group physical UNP ports or link aggregates into one logical domain.
- Once a port is assigned to a specific customer domain (see the **unp domain** command page**)**, classification rules associated with the same customer domain ID are applied only to UNP ports associated with the same domain ID.

Examples

```
-> unp domain 1
-> unp domain 2 description CustomerA
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp domain	Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.
show unp domain	Displays the customer domain ID configuration for the switch.

MIB Objects

```
alaDaUnpCustomerDomainTable
   alaDaUnpCustomerDomainId
   alaDaUnpCustomerDomainDesc
```

unp redirect pause-timer

Configures the global pause timer value for the switch. Use this command to configure the amount of time the switch filters traffic from a non-supplicant (non-802.1X device) on a UNP port. This is done to allow enough time for the switch to clear the authentication state of the non-supplicant, at which time the device is re-authenticated.

unp redirect pause-timer *seconds*

no redirect pause-timer

Syntax Definitions

seconds	The pause timer value. The valid range is 60–65535

Defaults

By default, the pause timer is set to zero.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to reset the pause time back to the default (timer no set).
- The pause timer is triggered when a Change of Authorization (COA) request is received that requires a VLAN change for a non-supplicant (non-802.1X device) *and* the port bounce action is not triggered for the device.
- During the pause time period, it is expected that the DHCP lease of the client IP in the old VLAN will expire and the client device will re-initiate DHCP resulting in new authentication and a UNP VLAN assignment.
- This command is used when configuring the switch to interact with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch Bring Your Own Devices (BYOD) solution.

Examples

```
-> unp redirect pause-timer 180
-> no unp redirect pause-timer
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp redirect port-bounce	Configures the port bounce action for a port or globally for the switch.
unp redirect proxy-server-port	Configures the HTTP proxy port number to use for redirection.
unp redirect allowed-name	Configures a list of additional IP addresses to which a host can access.
unp redirect-server	Configures an IP network address to allow HTTP traffic redirection.
show unp global configuration	Displays the global UNP parameter settings for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPRedirectPauseTimer
```

unp redirect proxy-server-port

Configures the HTTP proxy port number to use for redirection to the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) server.

unp redirect proxy-server-port *proxy_port*

no unp rediret proxy-server-port

Syntax Definitions

proxy_port	The HTTP proxy port number. The valid range is 1024–49151.

Defaults

By default, the redirect proxy port number is set to 8080 (traps HTTP 80, 8080, and 443).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to set the proxy port number back to the default (8080).
- Configuring the switch to interact with the UPAM or CPPM is done as part of the OmniSwitch implementation of the Bring Your Own Devices (BYOD) solution.

Examples

```
-> unp redirect proxy-server-port 8887
-> no unp redirect proxy-server-port
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp redirect port-bounce	Configures the port bounce action for a port or globally for the switch.
unp redirect pause-timer	Configures the global pause timer value for the switch.
unp redirect allowed-name	Configures a list of additional IP addresses to which a host can access.
unp redirect-server	Configures an IP network address to allow HTTP traffic redirection.
show unp global configuration	Displays the global UNP parameter settings for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
  alaDaUNPRedirectServerIP
```

unp redirect-server

Configures an IP network address or a Fully Qualified Domain Name (FQDN) to allow redirection of HTTP traffic to the Unified Policy Access Manager (UPAM) server or the ClearPass Policy Manager (CPPM) server. Specify the address or domain name that is associated with the dynamic URL returned from the UPAM or CPPM server.

unp redirect-server {*ip_address* | *domain_name***}**

no unp redirect-server

Syntax Definitions

ip_address	The IPv4 network address (e.g., 171.15.0.0) to which HTTP traffic is redirected.
domain_name	An FQDN (e.g., upam.com) to which HTTP traffic is redirected.

Defaults

By default, no redirect server IP address or FQDN is specified.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the redirect server IP or FQDN from the switch configuration.
- If the redirect server IP address or FQDN does not match the UPAM or CPPM server configuration, then redirection to the URL will not work. This provides additional security.
- Configuring the switch to interact with UPAM or CPPM is done as part of the OmniSwitch implementation of the Bring Your Own Devices (BYOD) solution.

Examples

```
-> unp redirect-server 10.0.0.20
-> no unp redirect-server
-> unp redirect-server upam.com
-> no unp redirect-server
```

Release History

Release 8.1.1; command was introduced.
Release 8.5R1; *domain_name* parameter added.

Related Commands

unp redirect port-bounce	Configures the port bounce action for a port or globally for the switch.
unp redirect pause-timer	Configures the global pause timer value for the switch
unp redirect proxy-server-port	Configures the HTTP proxy port number to use for redirection.
unp redirect allowed-name	Configures a list of additional IP addresses to which a host can access.
show unp global configuration	Displays the global UNP configuration for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
  alaDaUNPRedirectServerIPType
  alaDaUNPRedirectServerIP
```

unp redirect allowed-name

Configures a list of additional IP addresses to which a host can access. This allows traffic to reach additional subnets other than that of the Unified Policy Access Manager (UPAM) server or the ClearPass Policy Manager (CPPM) server.

unp redirect allowed-name *name* **ip-address** *ip_address* **ip-mask** *ip_mask*

no unp redirect allowed-name *name*

Syntax Definitions

name	Specify a name to assign to the allowed IP network address.
ip_address	An IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).
ip_mask	The IP subnet mask for the allowed IP network address.

Defaults

By default, no allowed IP addresses are configured.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IP address from the allowed list.
- Explicitly configure and append the allowed IP list to the built-in "restrictedPolicylist" policy list.

Examples

```
-> unp redirect allowed-name server2 ip-address 10.0.0.20 ip-mask 255.0.0.0
-> no unp redirect allowed-name server2
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp redirect port-bounce	Configures the port bounce action for a port or globally for the switch.
unp redirect pause-timer	Configures the global pause timer value for the switch
unp redirect proxy-server-port	Configures the HTTP proxy port number to use for redirection.
unp redirect-server	Configures an IP network address to allow HTTP traffic redirection.
show unp global configuration	Displays the global UNP configuration for the switch.

MIB Objects

```
alaDaUNPRedirectAllowedServerTable
  alaDaUNPRedirectAllowedServerName
  alaDaUNPRedirectAllowedServerIP
  alaDaUNPRedirectAllowedMaskIP
```

unp force-l3-learning

Configures the status of UNP Layer 3 learning on the specified UNP port or globally on all UNP ports. When this functionality is enabled and IP-based classification rules are configured on the switch, only Layer 3 packets are used to learn devices connected to UNP ports. Layer 2 packets are not used for learning devices.

unp [port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]] force-l3-learning [port-bounce]**

no unp [port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]] force-l3-learning [port-bounce]**

Syntax Definitions

*chassis/slot/port***[**-*port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number for a specific UNP link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).
port-bounce	Resets the context in which the user device is learned after the device is re-classified with a new IP address. This option is not supported on UNP link aggregates.

Defaults

By default, UNP Layer 3 learning is disabled and the port bounce action is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To disable Layer 3 learning for a specific port or link aggregate, use the **no** form of this command with the **port** or **linkagg** parameter. To globally disable Layer 3 learning, use the **no** form of this command without the **port** or **linkagg** parameter.
- When UNP Layer 3 learning is enabled and there is at least one IP-based classification rule configured, the first packet of the following types of packets is used to learn the device:
  - An IP packet with a non-zero source IP address.
  - A valid ARP/GARP request/reply.
  - DHCP packets, even if the source IP address is 0.0.0.0.

  However, the first packet of the following types of packets is *dropped* and not used to learn the device:
  - Layer 2 frames.
  - Invalid ARP/GARP request/reply (one with sender IP address 0.0.0.0 or 169.254.0.0/16).
  - IP packet with a source IP address of 0.0.0.0, except for DHCP packets where the source IP address is 0.0.0.0.
- When Layer 3 learning is enabled and a device is learned and assigned to a UNP profile, any subsequent change to the IP address for that device (for example, the device is assigned a leased IP address) will trigger UNP to re-classify the device based on the new IP address.

- When Layer 3 learning is enforced, the following users learned on a UNP port or link aggregate would not undergo IP reclassification:
  - 802.1x (supplicant) and MAC authenticated (non-supplicant).
  - Users learned through a non-IP-based classification rule that has a higher precedence over IP-based classification rules (such as any UNP extended classification rule, binding rule, MAC address rule, or MAC address range rule).
- When Layer 3 learning is enforced, the following users learned on a UNP port or link aggregate might undergo IP reclassification:
  - Users learned through a non-IP-based classification rule that has a lower precedence than IP-based classification rules (such as a VLAN rule).
  - IP-based classification rule.
- If the port bounce action is enabled for Layer 3 learning, IP reclassification for a user might result in obtaining a new UNP profile based on an IP-based classification rule, and the new UNP profile may assign a VLAN that is different from the initial UNP profile VLAN. If this occurs, the port would be toggled causing the user context to get flushed, and the subsequent packet from the user would then be used to relearn the user. It is assumed that user in this case would subsequently send either a valid ARP packet or an IP packet with a valid source IP address as the first packet, which would be used for re-learning the user directly into the final UNP profile.
- Note that the IP address update/change for an already learned UNP user can happen only when a valid ARP packet is sent from the user after the user is initially learned. As a result, Layer 3 enforcement relies on an ARP packet from the user.
- Whenever an additional port is configured as a UNP port , the Layer 3 learning status is derived from the global setting for the switch.
- When Layer 3 learning is changed at the global level, all port-level configurations are also changed unless a custom port template that configures this function is assigned to the port. For example, when Layer 3 learning is globally disabled, it is automatically disabled on any port that has Layer 3 learning enabled. However, if a port is assigned to a custom port template that enables this function, then the Layer 3 learning status for that port is not changed.
- The port-level setting of the Layer 3 learning function overrides the global setting for the switch. For example, if Layer 3 learning is globally disabled but enabled on port 1/1/20, then Layer 3 learning is active only on port 1/1/20.

Examples

```
-> unp force-l3-learning
-> unp force-l3-learning port-bounce
-> no unp force-l3-learning port-bounce
-> no unp force-l3-learning

-> unp port 1/1/20 force-l3-learning
-> unp port 1/1/20 force-l3-learning port-bounce
-> no unp port 1/1/20 force-l3-learning port-bounce
-> no unp port 1/1/20 force-l3-learning
```

Release History

Release 8.3.1; command was introduced.
Release 8.3.1.R02; **port**, **linkagg**, and **port-bounce** parameters added.

Related Commands

show unp global configuration	Displays the status of UNP Layer 3 learning for the switch.
show unp port config	Displays the status of port-level UNP Layer 3 learning.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPForceL3Learning
   alaDaUNPForceL3LearningPortBounce
alaDaUNPPortTable
   alaDaUNPPortForceL3Learning
   alaDaUNPPortForceL3LearningPortBounce
```

unp 802.1x-pass-through

Configures the global status of 802.1x pass through for the switch. When this functionality is enabled, 802.1x packets from supplicants attempting to authenticate are not processed on the local switch. Instead, the packets are passed along to another switch for authentication.

unp 802.1x-pass-through

no unp 802.1x-pass-through

Syntax Definitions

N/A

Defaults

By default, 802.1x pass through is disabled for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable 802.1x pass through for the switch.
- Enabling 802.1x pass through on a switch that has an existing UNP or LPS configuration is not recommended. This functionality is intended for a local or intermediate switch when the supplicant device requires authentication through an upstream switch.
- If 802.1x pass through is enabled on a switch that has an existing UNP or LPS configuration, consider the following:
  - 802.1x authentication, 802.1x authentication bypass, and MAC authentication allow EAP functionality is not supported on UNP ports.
  - The initial frame for unknown 802.1x traffic is learned on the switch. If the frame is learned in the forwarding mode, subsequent frames with the same source MAC address are passed through to the next switch. If the frame is learned in the filtering mode, subsequent frames with the same source MAC address are dropped and not passed through.

Examples

```
-> unp 802.1x-pass-through
-> no unp 802.1x-pass-through
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

show unp global configuration Displays the status of 802.1x pass through for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNP8021XPassThrough
```

unp ipv6-drop

Configures whether IPv6 packets received on UNP ports are learned or dropped. When this functionality is enabled, IPv6 packets are dropped by UNP on the local switch.

unp ipv6-drop

no unp ipv6-drop

Syntax Definitions

N/A

Defaults

By default, IPv6 packet drop is disabled. IPv6 packets are learned and processed by UNP.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to disable IPv6 packet drop for the switch.

Examples

```
-> unp ipv6-drop
-> no unp ipv6-drop
```

Release History

Release 8.5R2; command was introduced.

Related Commands

show unp global configuration Displays the status of IPv6 packet drop for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPIpv6Drop
```

unp ap-mode

Configures the global status of the Access Point (AP) mode. The global AP mode status determines the default AP mode status that is applied when a port or link aggregate is configured as a UNP bridge port. For example, if the global status is disabled, the port-level status defaults to disabled; if the global status is enabled, the port-level status defaults to enabled.

unp ap-mode {enable | disable}

Syntax Definitions

enable	Sets the AP mode default status to enabled.
disable	Sets the AP mode default status to disabled.

Defaults

By default, the AP mode is enabled for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Changing the global AP mode status at any given time is allowed but does not change the port-level status set for any existing UNP bridge ports. If the AP mode is disabled for the port, it remains disabled after the global status change; if the AP mode is enabled for the port, it remains enabled after the global status change and any devices or clients learned on the port are not disrupted.
- To change the AP mode status for a specific UNP bridge port, use the **unp port ap-mode** command.

Examples

```
-> unp ap-mode disable
-> unp ap-mode enable
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

unp port ap-mode	Configures AP mode functionality for a UNP bridge port.
show unp global configuration	Displays the status of UNP Layer 3 learning for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPApMode
```

unp mac-mobility

Configures the global status of MAC address mobility; any new UNP service profiles will inherit the global MAC mobility status when the profile is created. Enabling MAC address mobility for a UNP service profile supports VRRP router communication over a Shortest Path Bridging (SPB) service domain.

unp mac-mobility

no unp mac-mobility

Syntax Definitions

N/A

Defaults

By default, the global MAC address mobility status is disabled.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to globally disable UNP MAC address mobility.
- Although the MAC mobility status is configured for UNP profiles, it's functionality is supported only on profiles mapped to SPB services. SPB service-mapped profiles generate Service Access Points (SAPs) on which a VRRP router can communicate with other VRRP routers across the SPB service domain.
- When a new UNP service profile is created, the MAC mobility status for the profile defaults to the global value. For example, if the global status is enabled, then the new service profile status is set to enabled by default; if the global status is disabled, then the new service profile status is set to disabled by default.
- If the global MAC mobility status is changed at any given time, it will not affect the MAC mobility status of any existing UNP service profiles; the global setting only applies at the time a service profile is created. Any subsequent profiles created will default to the new global MAC mobility status.
- To change the MAC mobility status for a specific UNP service profile, use the **unp profile mac-mobility** command.

Examples

```
-> unp mac-mobility
-> no unp mac-mobility
```

Release History

Release 8.6R1; command was introduced.

Related Commands

unp profile mac-mobility	Configures the MAC mobility status for the specified UNP service profile.
show unp global configuration	Displays the status of MAC mobility for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPMacMobility
```

unp user flush

Performs a MAC address flush of Access Guardian users (devices learned on UNP ports) based on the specified port, link aggregate, authentication type, or MAC address.

unp user flush [port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]] [sap-id [linkagg]** *sap_id***] [service-id** *service_id***] [authentication-type {mac | 802.1x | none} [profile** *profile_name***] [mac-address** *mac_address***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
[linkagg] *sap_id*	A Service Access Point (SAP) ID. Use the optional **linkagg** parameter if the SAP ID is for a link aggregate.
service_id	A service ID.
mac	Clears only the MAC authenticated users.
802.1x	Clears only the 802.1X authenticated users.
none	Clears only the users that have not been authenticated.
mac_address	A MAC address (e.g., 00:00:39:59:f1:0c).
profile_name	The name of an existing UNP profile.

Defaults

By default, all MAC addresses learned on all UNP ports are flushed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **port** or **linkagg** parameter to flush users on a specific port or link aggregate.
- Use the **sap-id** parameter to flush users learned on a specific SAP. A SAP ID is comprised of a device-facing port or link aggregate (referred to as a service access port) and an encapsulation value that is used to identify the type of device traffic to map to the associated service.
- Use the **service-id** parameter to flush users learned on a specific service.
- Use the **authentication-type** parameter with the **mac**, **802.1x**, or **none** options to flush users that were authenticated (MAC or 802.1X) or users that were not authenticated.
- Use the **mac-address** parameter to flush a specific device.

- Use the **profile** parameter to flush all users associated with the specified profile name. Combine this parameter with the **mac-address** parameter to flush a specific user associated with the specified profile name.
- Combine the **sap-id** or **service-id** parameter with the **profile** parameter option to flush only users on the SAP or service that are classified into the specified profile.
- Combine the **sap-id** or **service-id** parameter with the **authentication-type** parameter option to flush only users on the SAP or service that were authenticated with the specified authentication type.

Examples

```
-> unp user flush
-> unp user flush port 1/1/6
-> unp user flush linkagg 10
-> unp user flush sap-id 1/1/2:50
-> unp user flush service-id 10
-> unp user flush authentication-type mac
-> unp user flush mac-address 00:11:22:33:44:55
-> unp user flush profile unp1-vlan
-> unp user flush profile unp1-vlan mac-address 00:da:95:11:22:01
```

Release History

Release 8.3.1; command was introduced.

Related Commands

show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPUserFlushTable
   alaDaUNPUserFlushIndex
   alaDaUNPUserFlushComplete
   alaDaUNPUserFlushAuthType
   alaDaUNPUserFlushMacAddress
   alaDaUNPUserFlushProfile
   alaDaUNPUserFlushPortStart
   alaDaUNPUserFlushPortEnd
   alaDaUNPUserFlushSapIDIfIndex
   alaDaUNPUserFlushSapIDEncapVal
   alaDaUNPUserFlushServiceID
```

unp profile

Configures a classification profile that is used to provide role-based access to the switch. This type of profile determines the VLAN or service a device can join and applies any additional profile-defined attributes to the device.

When a profile is created with this command, the base command (**unp profile** *profile_name*) may be used with other command keywords to define attributes for the specified profile. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

unp profile *profile_name*
[qos-policy-list *list_name***]**
[location-policy *policy_name***]**
[period-policy *policy_name***]**
[captive-portal-authentication]
[captive-portal-profile *profile_name***]**
[kerberos-authentication]
[authentication-flag]
[mobile-tag]
[maximum ingress-bandwidth *bps***[k | m]]**
[maximum egress-bandwidth *bps***[k | m]]**
[maximum ingress-depth *bps***]**
[maximum egress-depth *bps***]**
[inactivity-interval *seconds***]**
[mac-mobility]
[saa-profile *profile_name***]**

no unp profile *profile_name*

Syntax Definitions

profile_name	The name to assign to the UNP classification profile.

Defaults

When a profile is created without specifying any parameter values, the profile parameters are set to the following default values:

parameter	default
qos-policy-list *list_name*	No list assigned
location-policy	No policy assigned
period-policy	No policy assigned
captive-portal-authentication	disabled
captive-portal-profile	No profile assigned
kerberos-authentication	disabled
authentication-flag	disabled

parameter	default
mobile-tag	disabled
maximum ingress-bandwidth *bps***[k | m]**	None
maximum egress-bandwidth *bps***[k | m]**	None
maximum ingress-depth *bps*	None
maximum egress-depth *bps*	None
inactivity-interval *seconds*	10
mac-mobility	disabled
saa-profile *profile_name*	No profile assigned

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a profile from the switch configuration.
- Profiles are applied only to traffic received on UNP bridge and access ports or link aggregates.
- After a profile is created, use the **unp profile map** command to map the profile to a VLAN or service.
  - If the profile is mapped to a VLAN, the profile is used to classify traffic received on UNP bridge ports.
  - If the profile is mapped to a service (SPB, VXLAN, or static), the profile is used to classify traffic received on UNP access ports.
- Any configuration change to a profile will flush all MAC addresses learned on that profile.

Examples

```
-> unp profile unp-prof1
-> no unp profile unp-prof1
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile qos-policy-list	Assigns a QoS policy list to an existing profile.
unp profile location-policy	Assigns a UNP location policy to the specified profile.
unp profile period-policy	Assigns a UNP time-based policy to the specified profile.
unp profile captive-portal-authentication	Configures the status of Captive Portal authentication for the specified profile.
unp profile captive-portal-profile	Assigns a Captive Portal configuration to the specified profile.
unp profile kerberos-authentication	Configures the status of Kerberos snooping for the specified profile.
unp profile authentication-flag	Configures whether the specified profile only allows authenticated devices into the profile.
unp profile mobile-tag	Configures whether a tagged VLAN-port association is created for a device port that is classified into the specified profile.
unp profile maximum-ingress-bandwidth	Configures a maximum ingress bandwidth value that is applied to UNP ports associated with the specified profile.
unp profile maximum-egress-bandwidth	Configures a maximum egress bandwidth value that is applied to UNP ports associated with the specified profile.
unp profile maximum-ingress-depth	Configures a maximum ingress depth value that is applied to UNP ports associated with the specified profile.
unp profile maximum-egress-depth	Configures a maximum egress depth value that is applied to UNP ports associated with the specified profile.
unp profile inactivity-interval	Configures the inactivity interval timer for the specified profile.
unp profile mac-mobility	Configures the MAC address mobility status for the specified UNP service profile to support VRRP router communication over an SPB service domain.
unp profile saa-profile	Assigns an existing Service Assurance Agent (SAA) profile to the specified profile.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
```

unp profile qos-policy-list

Configures the QoS policy list attribute for the specified profile. Use this command to assign the name of an existing QoS policy list to the profile. A policy list contains QoS policy rules/ACLs that are applied to devices classified with the associated profile.

unp profile *profile_name* **qos-policy-list** *list_name*

no unp profile *profile_name* **qos-policy-list**

Syntax Definitions

profile_name	The name of a UNP profile.
list_name	The name of a QoS policy list to associate with the specified UNP.

Defaults

By default, no profile attributes are enabled or defined when the profile is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the QoS list name from the profile configuration.
- Specifying a QoS policy list name that is inactive or does not already exist in the switch configuration is allowed. However, the list will remain inactive for the UNP until the list is enabled or configured using the QoS **policy list** command.
- The QoS policy list is used to define the initial role for any UNP user learned in the profile.

Examples

```
-> unp profile unp-prof1 qos-policy-list unp-list1
-> no unp profile unp-prof1 qos-policy-list unp-list2
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP classification profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
policy list	Configures a QoS policy list.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileQoSPolicy
```

unp profile location-policy

Configures the location policy attribute for the specified profile. Use this command to assign the name of an existing UNP location policy to a profile. This type of policy defines criteria (such as the slot/port, system name and location) to determine if a device is accessing the network from a valid location.

unp profile *profile_name* **location-policy** *policy_name*

no unp profile *profile_name* **location-policy**

Syntax Definitions

profile_name	The name of a UNP profile.
policy_name	The name of an existing UNP location policy.

Defaults

By default, no profile attributes are enabled or defined when the profile is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the location policy name from the profile configuration.
- The location policy name specified with this command must already exist in the switch configuration.
- Profile location and time period policies are configurable on the switch or on the RADIUS server. If the policies are configured on both the switch and the RADIUS server, then the switch policies take precedence.
- If a UNP device does not meet the criteria applied through the location policy, the device role is changed to unauthorized.

Examples

```
-> unp profile unp-prof1 location-policy alu-na
-> no unp profile unp-prof1 location-policy
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
unp policy validity-location	Configures a UNP location policy.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileLocationPolicy
```

unp profile period-policy

Configures the period policy attribute for the specified profile. Use this command to assign the name of an existing UNP period policy to a profile. This type of policy specifies the days and times during which a device can access the network.

unp profile *profile_name* **period-policy** *policy_name*

no unp profile *profile_name* **period-policy**

Syntax Definitions

profile_name	The name of a UNP profile.
policy_name	The name of an existing UNP period policy.

Defaults

By default, no profile attributes are enabled or defined when the profile is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the period policy name from the profile configuration.
- The period policy name specified with this command must already exist in the switch configuration.
- Profile location and time period policies are configurable on the switch or on the RADIUS server. If the policies are configured on both the switch and the RADIUS server, then the switch policies take precedence.
- If a UNP device does not meet the criteria applied through the period policy, the device role is changed to unauthorized.

Examples

```
-> unp profile unp-prof1 period-policy office-time
-> no unp profile unp-prof1 period-policy
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
unp policy validity-period	Configures a UNP period policy.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfilePeriodPolicy
```

unp profile captive-portal-authentication

Configures the status of Captive Portal (CP) authentication for the specified UNP profile. When enabled, the Captive Portal authentication process is triggered for devices classified into the profile.

unp profile *profile_name* **captive-portal-authentication**

no unp profile *profile_name* **captive-portal-authentication**

Syntax Definitions

profile_name	The name of a UNP profile.

Defaults

By default, Captive Portal authentication is disabled for the profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- Use the **no** form of this command to disable Captive Portal authentication for the profile configuration.
- When CP authentication is enabled, the UNP user is assigned an implicit CP pre-login role to facilitate the CP authentication process with the configured CP RADIUS server.
- The CP profile associated with the UNP profile defines the CP RADIUS server to use for the CP authentication process. If a CP profile is not associated with the UNP profile, then the server defined in the global CP configuration for the switch is used instead.
- If CP authentication for the device is successful, the user role is automatically changed according to the CP pass policy list returned from the RADIUS server if it is the highest precedence role known for the user.
- If CP authentication for the device fails, the user role will be changed to the last known highest precedence role for the user.
- When successful CP authentication results in assigning the UNP user to a different profile, CP authentication does not need to be enabled for that profile. For example, if the user is initially assigned to a “Guest” profile and successful CP authentication assigns the user to the “Admin” profile, CP authentication must be enabled on the “Guest” profile but does not have to be enabled on the “Admin” profile.
- When CP authentication is disabled for the profile, BYOD redirection is automatically made available to devices assigned to the profile. When CP authentication is enabled, CP is enforced and BYOD redirection is not available.

Examples

```
-> unp profile unp-prof1 captive-portal-authentication
-> no unp profile unp-prof1 captive-portal-authentication
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileCPortalAuthentication
```

unp profile captive-portal-profile

Configures the Captive Portal (CP) profile attribute for the specified profile. Use this command to assign the name of an existing CP profile to a profile. This type of profile defines a CP configuration that is applied to devices when CP authentication is enabled for the profile.

unp profile *profile_name* **captive-portal-profile** *cp_profile_name*

no unp profile *profile_name* **captive-portal-profile**

Syntax Definitions

profile_name	The name of a UNP profile.
cp_profile_name	The name of an existing UNP Captive Portal profile.

Defaults

By default, no CP profile is assigned to a profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- Use the **no** form of this command to remove the CP profile name from the profile configuration.
- The CP profile name specified with this command must already exist in the switch configuration.
- The configuration defined in the CP profile overrides the global CP configuration for the switch.

Examples

```
-> unp profile unp-prof1 captive-portal-profile cp-prof
-> no unp profile unp-prof1 captive-portal-profile
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
captive-portal-profile	Configures a Captive Portal profile.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileCPortalProfile
```

unp profile kerberos-authentication

Enables or disables Kerberos snooping on UNP profile.

unp profile *profile_name* **kerberos-authentication**

no unp profile *profile_name* **kerberos-authentication**

Syntax Definitions

profile_name	The name of a UNP profile.

Defaults

By default, Kerberos is disabled on UNP profile.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable Kerberos snooping on the UNP profile.
- When Kerberos is disabled on the UNP profile, all users learned in that profile are deleted.
- Although the status of Kerberos snooping is configurable for UNP profiles, it's functionality is supported only on profiles mapped to a VLAN.
- Kerberos is an L3 authentication. It will be available only after successful L2 authentication.
- Kerberos snooping will work only when the switch has at least one Kerberos server IP address configured.

Examples

```
-> unp profile p1 kerberos-authentication
-> no unp profile p1 kerberos-authentication
```

Release History

Release 8.6R2; command introduced.

Related Commands

kerberos inactivity-timer	Configures the global inactivity timer for Kerberos users.
show kerberos configuration	Displays the Kerberos global configuration.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileKerberosAuthentication
   alaDaUNPProfileRowStatus
```

unp profile authentication-flag

Configures the authentication flag status for the specified UNP profile. When enabled, only devices successfully authenticated are classified into the profile.

unp profile *profile_name* **authentication-flag**

no unp profile *profile_name* **authentication-flag**

Syntax Definitions

profile_name	The name of a UNP profile.

Defaults

By default, the authentication flag is disabled for the profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the authentication flag for the profile configuration.
- When the authentication flag is enabled for a profile, devices that did not pass L2 authentication (802.1X or MAC) are not allowed into the profile. However, other configured classification options are applied to such devices to determine the appropriate network access control for that device.

Examples

```
-> unp profile unp-prof1 authentication-flag
-> no unp profile unp-prof1 authentication-flag
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileAuthenticationFlag
```

unp profile mobile-tag

Configures the mobile tag status for the specified UNP profile. When enabled, the first user that is learned on a UNP port and classified into the specified UNP profile will cause the UNP port to be added as a tagged member of the VLAN associated with the profile. If the profile is mapped to a service, a tagged virtual port association is created.

unp profile *profile_name* **mobile-tag**

no unp profile *profile_name* **mobile-tag**

Syntax Definitions

profile_name	The name of a UNP profile.

Defaults

By default, the mobile tag status is disabled for the profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the mobile tag status for the profile configuration.
- When the mobile tag status is disabled for a profile, any user device classified into the profile will remain learned in that profile. In this case, the tagged/untagged VLAN-port association would be determined based on the user traffic which was learned as tagged or untagged, respectively.
- If the device port is already an untagged member of the VLAN associated with the profile, then a tagged association is not created.

Examples

```
-> unp profile unp-prof1 mobile-tag
-> no unp profile unp-prof1 mobile-tag
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
show unp profile	Displays the UNP profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileMobileTag
```

unp profile maximum-ingress-bandwidth

Configures the maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the specified profile.

unp profile *profile_name* **maximum-ingress-bandwidth** *bps***[k | m]**

no unp profile *profile_name* **maximum-ingress-bandwidth**

Syntax Definitions

profile_name	The name of a UNP profile.
*bps***[k | m]**	The maximum amount of bandwidth, in bits-per-second. The valid range is 0–10485760. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m**).

Defaults

By default, the maximum ingress bandwidth value is not defined for the profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the maximum ingress bandwidth value for the specified profile. If a maximum ingress depth value is set for the same profile, then both the maximum ingress bandwidth and depth values must be removed together (on the same command line).
- If the maximum ingress bandwidth value is specified as an integer without an abbreviated unit designation, the value is applied in Kbps by default. For example, if the number **10** is specified, **10K** is the value applied.
- If the maximum ingress bandwidth value is set to zero, then all ingress traffic is allowed on the UNP port.
- The maximum ingress bandwidth, egress bandwidth, and depth values are applied to the port of a user device that is classified into the specified profile.
  - If multiple user devices are classified into different profiles but learned on the same UNP port, the bandwidth parameter values obtained for the last user learned are applied on the port. Parameter values applied through previously learned users are overwritten.
  - Bandwidth parameter values are *not* applied to UNP link aggregates that are assigned to the profile.

Examples

```
-> unp profile unp-prof1 maximum-ingress-bandwidth 100
-> unp profile unp-prof1 maximum-ingress-bandwidth 10m
-> no unp profile unp-prof1 maximum-ingress-bandwidth

-> unp profile unp-prof1 maximum-ingress-bandwidth 100
-> unp profile unp-prof1 maximum-ingress-depth 50
-> no unp profile unp-prof1 maximum-ingress-bandwidth maximum-ingress-depth
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
unp profile maximum-ingress-depth	Configures how much the traffic can burst over the maximum ingress bandwidth rate.
show unp profile	Displays the profile configuration for the switch.
show unp port bandwidth	Displays the bandwidth parameter values applied to a UNP port or link aggregate.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileMaxIngressBandwidth
```

unp profile maximum-egress-bandwidth

Configures the maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the specified profile.

unp profile *profile_name* **maximum-egress-bandwidth** *bps***[k | m]**

no unp profile *profile_name* **maximum-egress-bandwidth**

Syntax Definitions

profile_name	The name of a UNP profile.
*bps***[k | m]**	The maximum amount of bandwidth, in bits-per-second. The valid range is 0–10485760. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m**).

Defaults

By default, the maximum egress bandwidth value is not defined for the profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the maximum egress bandwidth value for the specified profile. If a maximum egress depth value is set for the same profile, then both the maximum egress bandwidth and depth values must be removed together (on the same command line).
- If the maximum egress bandwidth value is specified as an integer without an abbreviated unit designation, the value is applied in Kbps by default. For example, if the number **10** is specified, **10K** is the value applied.
- If the maximum egress bandwidth value is set to zero, then all egress traffic is allowed on the UNP port.
- The maximum ingress bandwidth, egress bandwidth, and depth values are applied to the port of a user device that is classified into the specified profile.
  - If multiple user devices are classified into different profiles but learned on the same UNP port, the bandwidth parameter values obtained for the last user learned are applied on the port. Parameter values applied through previously learned users are overwritten.
  - Bandwidth parameter values are *not* applied to UNP link aggregates that are assigned to the profile.

Examples

```
-> unp profile unp-prof1 maximum-egress-bandwidth 100
-> unp profile unp-prof1 maximum-egress-bandwidth 10m
-> no unp profile unp-prof1 maximum-egress-bandwidth

-> unp profile unp-prof1 maximum-egress-bandwidth 100
-> unp profile unp-prof1 maximum-egress-depth 50
-> no unp profile unp-prof1 maximum-egress-bandwidth maximum-egress-depth
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
unp profile maximum-egress-depth	Configures how much the traffic can burst over the maximum egress bandwidth rate.
show unp profile	Displays the profile configuration for the switch.
show unp port bandwidth	Displays the bandwidth parameter values applied to a UNP port or link aggregate.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileMaxEgressBandwidth
```

unp profile maximum-ingress-depth

Configures the maximum ingress queue depth or bucket size assigned to each port that is associated with the specified UNP profile. The depth value is configured in bytes and is used for traffic metering. The queue depth or bucket size determines the amount of buffers allocated to the UNP port. When the queue or bucket size is reached, the switch starts dropping packets.

unp profile *profile_name* **maximum-ingress-depth** *bytes*

no unp profile *profile_name* **maximum-ingress-depth**

Syntax Definitions

profile_name	The name of a UNP profile.
bytes	The maximum ingress depth value in bytes. The valid range is 0–16384.

Defaults

By default, the maximum ingress depth value is determined by dividing the maximum ingress bandwidth value by 25. If the result of this calculation is 0 or 1, then 2K is used as the ingress depth value.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the maximum ingress depth value from the profile.
- The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter. When the ingress depth value is reached, the switch starts to drop packets.
- Configure the maximum ingress bandwidth rate (**unp profile maximum-ingress-bandwidth**) before attempting to set the maximum ingress depth value.
- The maximum ingress bandwidth and depth values are applied to the port of a user device that is classified into the specified profile.
  - If multiple user devices are classified into different profiles but learned on the same UNP port, the bandwidth parameter values obtained for the last user learned are applied on the port. Parameter values applied through previously learned users are overwritten.
  - Bandwidth parameter values are *not* applied to UNP link aggregates that are assigned to the profile.

Examples

```
-> unp profile unp-prof1 maximum-ingress-bandwidth 10
-> unp profile unp-prof1 maximum-ingress-depth 5
-> no unp profile unp-prof1 maximum-ingress-depth
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
unp profile maximum-ingress-bandwidth	Configures the maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the specified profile.
show unp profile	Displays the profile configuration for the switch.
show unp port bandwidth	Displays the bandwidth parameter values applied to a UNP port or link aggregate.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileMaxIngressDepth
```

unp profile maximum-egress-depth

Configures the maximum ingress queue depth or bucket size assigned to each port that is associated with the specified UNP profile. The depth value is configured in bytes and is used for traffic metering. The queue depth or bucket size determines the amount of buffers allocated to the UNP port. When the queue or bucket size is reached, the switch starts dropping packets.

unp profile *profile_name* **maximum-egress-depth** *bytes*

no unp profile *profile_name* **maximum-egress-depth**

Syntax Definitions

profile_name	The name of a UNP profile.
bytes	The maximum egress depth value in bytes. The valid range is 0–16384.

Defaults

By default, the maximum egress depth value is determined by dividing the maximum ingress bandwidth value by 25. If the result of this calculation is 0 or 1, then 2K is used as the ingress depth value.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the maximum egress depth value from the profile.
- The maximum egress depth value is configured in conjunction with the maximum egress bandwidth parameter. When the egress depth value is reached, the switch starts to drop packets.
- Configure the maximum egress bandwidth rate (**unp profile maximum-egress-bandwidth**) before attempting to set the maximum egress depth value.
- The maximum egress bandwidth and depth values are applied to the port of a user device that is classified into the specified profile.
  - If multiple user devices are classified into different profiles but learned on the same UNP port, the bandwidth parameter values obtained for the last user learned are applied on the port. Parameter values applied through previously learned users are overwritten.
  - Bandwidth parameter values are *not* applied to UNP link aggregates that are assigned to the profile.

Examples

```
-> unp profile unp-prof1 maximum-egress-bandwidth 10
-> unp profile unp-prof1 maximum-egress-depth 5
-> no unp profile unp-prof1 maximum-egress-depth
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
unp profile maximum-egress-bandwidth	Configures the maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the specified UNP profile.
show unp profile	Displays the profile configuration for the switch.
show unp port bandwidth	Displays the bandwidth parameter values applied to a UNP port or link aggregate.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileMaxEgressDepth
```

unp profile inactivity-interval

Configures whether or not an authenticated device is automatically logged out of the network after a specific period of inactivity (MAC address for the device has aged out). This timer value applies only to devices learned in the specified profile.

unp profile *profile_name* **inactivity-interval** *seconds*

Syntax Definitions

profile_name	The name of a UNP profile.
seconds	The inactivity timer value. The valid range is 10 to 600 seconds.

Defaults

By default, the inactivity interval value is set to 10 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Make sure the configured inactivity interval time is set to a value greater than the MAC address aging time for the switch.
- When a specific time is configured for the inactivity interval timer, the device is not logged out of the network if the MAC address aging time expires before the configured timer value.
- When the inactivity interval time is changed for the profile, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- If a user undergoes MAC authentication and then secondary Captive Portal authentication, the higher of the two inactivity logout timer values returned is applied to the device.
- An inactivity logout timer value is also configurable through authentication, authorization, and accounting (AAA) commands. The value set through the AAA commands takes precedence over the inactivity interval value set for the UNP.

Examples

```
-> unp profile unp-prof1 inactivity-interval 500
-> unp profile unp-prof1 inactivity-interval 10
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileInactivityInterval
```

unp profile mac-mobility

Configures the MAC address mobility status for the specified UNP service profile. Enable MAC address mobility for a UNP service profile to support VRRP router communication over an SPB service domain.

unp profile *profile_name* **mac-mobility**

no unp profile *profile_name* **mac-mobility**

Syntax Definitions

profile_name	The name of a UNP profile that is mapped to SPB service parameters.

Defaults

By default, the MAC mobility status for the SPB service-mapped profile is set to the global MAC mobility status when the profile is created.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the MAC mobility status for the profile configuration.
- When the MAC mobility status is disabled for a profile, VRRP MAC address movement that is required for the VRRP master/slave election process is disrupted. This may cause a VRRP configuration to generate two VRRP masters within the SPB service domain.
- Although the MAC mobility status is configured for UNP profiles, it's functionality is supported only on profiles mapped to SPB services. SPB service-mapped profiles generate Service Access Points (SAPs) on which a VRRP router can communicate with other VRRP routers across the SPB service domain.
- To support VRRP router communication over an SPB service domain, the following configuration is required:
  - Enable MAC address mobility for the SPB service-mapped UNP profile.
  - Assign the service profile to a UNP access port to create a persistent UNP SAP on which a VRRP router will communicate. A persistent SAP does not age out and will ensure an uninterrupted flow of VRRP advertisements between the VRRP master and slave routers.

Examples

```
-> unp profile unp-prof1 mac-mobility
-> no unp profile unp-prof1 mac-mobility
```

Release History

Release 8.6R1; command was introduced.

Related Commands

unp mac-mobility	Configures the global MAC mobility status for the switch.
unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
unp profile map service-type spb	Configures the mapping of SPB service parameters to the specified UNP profile. The service parameter values are used to define an SPB SAP on which profile traffic is forwarded.
show unp profile	Displays the UNP profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileMacMobility
```

unp profile saa-profile

Assigns a Service Assurance Agent (SAA) profile to the specified UNP profile. Although an SAA profile can be assigned to a UNP profile with this command, an SAA profile is mainly used by the OmniVista network management application to monitor connections between virtual machines (VMs) in a data center network.

unp profile *profile_name* **saa-profile** *profile_name*

no unp profile *profile_name* **saa-profile**

Syntax Definitions

profile *profile_name*	The name of a UNP profile.
saa-profile *profile_name*	The name of the SAA profile to assign to the UNP profile.

Defaults

By default, no SAA profile is assigned to a UNP profile.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove an SAA profile assignment from a UNP profile configuration.
- The SAA profile specified with this command must already exist in the switch configuration.

Examples

```
-> unp profile unp-prof1 saa-profile saa1
-> no unp profile unp-prof1 saa-profile
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
unp saa-profile	Configures an SAA profile.
show unp saa-profile	Displays the SAA profile configuration for the switch.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileSaaProfile
```

unp profile map vlan

Configures the mapping of a standard VLAN to a UNP profile. When a device is assigned to a profile through authentication or classification, the device and the port on which the device was learned are dynamically assigned to the VLAN that is mapped to the profile.

unp profile *profile_name* **map vlan** *vlan_id*

Syntax Definitions

profile_name	The name of an existing UNP profile.
vlan_id	The VLAN ID number to associate with the specified profile name. Devices assigned to the profile are assigned to the associated VLAN.

Defaults

By default, no mapping configuration is applied to a profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Removing a VLAN mapping configuration requires deleting the entire profile from the switch configuration (**no unp profile** *profile_name*).
- The VLAN associated with a profile must already exist in the switch configuration, unless one of the following conditions occur:
  - The dynamic VLAN configuration functionality is enabled for the switch.
  - The VLAN mapping to a profile is done when the switch boots up.
- Configuring a new VLAN mapping for a profile will overwrite the existing VLAN mapping for that profile. Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.
- Only one type of profile mapping (VLAN, SPB, VXLAN, or static) is associated with a profile at any given time.
- If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.
- If a profile is mapped to SPB, VXLAN, or static service parameters, then the profile is applied to traffic received on UNP access ports.

Examples

```
-> unp profile unp1-vlan map vlan 10
-> no unp profile unp1-vlan
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile.
unp dynamic-vlan-configuration	Configures the global UNP status for dynamic VLAN configuration.
unp profile map service-type spb	Maps SPB parameters to a profile. The parameters are used for creating an SPB service access point (SAP) to forward profile traffic.
unp profile map service-type vxlan	Maps VXLAN parameters to a profile. The parameters are used for creating a VXLAN service access point (SAP) to forward profile traffic.
unp profile map service-type static	Maps an existing SPB or VXLAN service ID to a profile.
show unp profile map	Displays the VLAN or service mapping configuration assigned to a UNP profile.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
alaDaUNPProfileMapVlanTable
   alaDaUNPProfileMapVlanVlanID
```

unp profile map service-type spb

Configures the mapping of Shortest Path Bridging (SPB) parameters to the specified UNP profile. When a device is dynamically assigned to the profile through authentication or classification, an SPB service access point (SAP) is automatically created using the specified profile parameters. Traffic from the device is then forwarded on the SAP.

unp profile *profile_name* **map service-type spb tag-value {0 |** *qtag* | *outer_qtag:inner_qtag}* **isid** *instance_id* **bvlan** *bvlan_id* **[multicast-mode {headend | tandem}] [vlan-xlation] [igmp-snooping [profile {default |** *ipms_profile***}] [mld-snooping [profile {default |** *ipms_profile***}]**

no unp profile *profile_name* **map service-type spb [vlan-xlation] [igmp-snooping [profile]] [mld-snooping [profile]]**

Syntax Definitions

profile_name	The name of an existing UNP profile.
0	Use VLAN tag information from classified traffic to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
qtag	The outer VLAN ID tag to use when creating a SAP for single-tagged traffic.
outer_qtag:inner_qtag	An outer VLAN ID tag and an inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
instance_id	A service instance identifier (I-SID) that is used to identify an SPB service in a provider backbone bridge (PBB) network. The valid range is 256–16777214.
bvlan_id	The VLAN ID number of an existing SPB backbone VLAN (BVLAN).
headend	Specifies the head-end replication mode for the service associated with this UNP.
tandem	Specifies the tandem replication mode for the service associated with this UNP.
vlan-translation	Configures egress VLAN translation for the service associated with this UNP.
igmp-snooping	Configures IGMP snooping for the service associated with this UNP.
mld-snooping	Configures MLD snooping for the service associated with this UNP.
ipms_profile_name	The name of an optional IP Multicast Switching profile to use when IGMP or MLD snooping is enabled.
default	Use default IPMS profile settings for IGMP or MLD snooping.

Defaults

By default, no mapping configuration is applied to a profile. When the SPB mapping is configured, the following default values are applied for the optional parameters:

parameter	default
multicast-mode {headend | tandem}	headend

parameter	default
vlan-xlation	disabled
igmp-snooping	disabled
mld-snooping	disabled
default | *ipms_profile_name*	default

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable VLAN translation, IGMP snooping, and MLD snooping for the UNP service profile. To remove any other SPB mapping parameter requires deleting the entire profile from the switch configuration (**no unp profile** *profile_name*).
- Configuring a new SPB mapping for a profile will overwrite the existing SPB mapping for that profile.
- Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.
- Only one type of profile mapping (VLAN, SPB, VXLAN, or static) is associated with a profile at any given time.
- If a profile is mapped to SPB, VXLAN, or static service parameters, then the profile is applied to traffic received on UNP access ports.
- If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.
- The **tag-value** parameter specifies the VLAN tag values that are used to create the SAP to which profile traffic is mapped. The SAP is then bound to the SPB service that is dynamically created based on the specified I-SID and BVLAN values.
- Consider the following when configuring the profile tag value:
  - If the tag value is set to zero, the SAP for the classified traffic is created using the VLAN tags of the traffic. For example, a SAP with an encapsulation value set to 1/12:5 is created when classified traffic received on port 1/12 is single-tagged with VLAN ID 5.
  - Enabling the trust VLAN tag option for the UNP service port triggers the same functionality as setting the service profile tag value to zero. In both cases, the VLAN tags of the classified traffic are used to specify the encapsulation value of the SAP to which the traffic is mapped.
  - If the trust VLAN tag option is disabled for the UNP port and the service profile tag value is *not* set to zero (for example, **tag-value** 10), the VLAN tag values of the classified traffic are compared to the configured profile tag value. If the traffic tag values match the profile tag value, the traffic is mapped to the appropriate SAP. If the traffic tags do not match, traffic is not mapped to a SAP.
- UNP first checks the switch configuration to see if a SAP already exists for the expected VLAN tag value (CVLAN tags) and I-SID. If a SAP already exists, the MAC addresses are learned on that SAP. If the SAP does not exist, the switch dynamically creates one for the profile traffic.
- If the I-SID specified with this command does not exist in the switch configuration, the switch will dynamically create the expected service and then the SAP as needed.
- The BVLAN ID specified with this command must already exist in the switch configuration.

- Dynamically creating services and related SAPs is subject to available switch resources. If an attempt to dynamically create a service or SAP fails, the MAC addresses classified for the service profile are learned as filtering.
- When an SPB service is configured to use the head-end multicast mode, a non-unicast packet received on an SPB access port is replicated once for each receiver in the provider backbone bridge (PBB) network using its unicast base MAC (BMAC) address.
- When an SPB service is configured to use the tandem multicast mode, a non-unicast packet received on an SPB access port is replicated once at each node using the multicast group address.
- Enabling VLAN translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled.
- When configuring the IGMP and MLD snooping mapping parameters, it is necessary to also configure the VLAN translation and multicast mode status for the profile mapping.

Examples

```
-> unp profile unp1-spb map service-type spb tag-value 10 isid 1510 bvlan 4001
-> unp profile unp2-spb map service-type spb tag-value 20 isid 1520 bvlan 4002
multicast-mode tandem vlan-xlation
-> unp profile unp3-spb map service-type spb tag-value 30 isid 1530 bvlan 4003
vlan-xlation multicast-mode headend igmp-snooping mld-snooping
-> unp profile unp4-spb map service-type spb tag-value 40 isid 1540 bvlan 4004
vlan-xlation multicast-mode headend igmp-snooping profile ipms-prof1
-> unp profile unp4-spb map service-type spb tag-value 40 isid 1540 bvlan 4004
vlan-xlation multicast-mode headend mld-snooping profile default

-> no unp profile unp1-spb
-> no unp profile unp2-spb map service-type spb vlan-xlation
-> no unp profile unp3-spb map service-type igmp-snooping
-> no unp profile unp3-spb map service-type mld-snooping
-> no unp profile unp4-spb map service-type mld-snooping profile
-> no unp profile unp4-spb map service-type mld-snooping
```

Release History

Release 8.3.1; command was introduced.
Release 8.6R1; **igmp-snooping** and **mld-snooping** parameters added.

Related Commands

unp profile	Configures a UNP profile.
unp profile map vlan	Maps VLAN IDs to a UNP profile. Traffic assigned to the profile is forwarded on the associated VLAN IDs.
unp profile map service-type vxlan	Maps VXLAN parameters to a profile. The parameters are used for creating a VXLAN service access point (SAP) to forward profile traffic.
unp profile map service-type static	Maps an existing SPB or VXLAN service ID to a profile.
show unp profile map	Displays the VLAN or service mapping configuration for the profile.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
alaDaUNPProfileMapSpbTable
   alaDaUNPProfileMapSpbEncapVal
   alaDaUNPProfileMapSpbIsid
   alaDaUNPProfileMapSpbBVlan
   alaDaUNPProfileMapSpbMulticastMode
   alaDaUNPProfileMapSpbVlanXlation
   alaDaUNPProfileMapSpbIgmpSnooping
   alaDaUNPProfileMapSpbIgmpProfile
   alaDaUNPProfileMapSpbMldSnooping
   alaDaUNPProfileMapSpbMldProfile
```

unp profile map service-type vxlan

Configures the mapping of Virtual eXtensible LAN (VXLAN) parameters to the specified UNP profile. When a device is dynamically assigned to the profile through authentication or classification, a VXLAN service access point (SAP) is automatically created using the specified profile parameters. Traffic from the device is then forwarded on the SAP.

unp profile *profile_name* **map service-type vxlan tag-value {0 |** *qtag* | *outer_qtag:inner_qtag***} vnid** *vxlan_id* **{far-end-ip-list** *ip_list_name* **[multicast-group** *mc_group_address***] | multicast-group** *mc_group_address* **[far-end-ip-list** *ip_list_name***]} [multicast-mode [tandem | headend | hybrid] [vlan-xlation]**

no unp profile *profile_name* **map service-type vxlan [far-end-ip-list | multicast-group | vlan-xlation]**

Syntax Definitions

profile_name	The name of an existing UNP profile.
0	Use VLAN tag information from classified traffic to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
qtag	The outer VLAN ID tag to use when creating a SAP for single-tagged traffic.
outer_qtag:inner_qtag	An outer VLAN ID tag and an inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
vxlan_id	The VXLAN network identifier that identifies the VLAN segment form where the frames originate. This value is used to create the VXLAN service that is required to dynamically create the SAP.
ip_list_name	The name of an existing list that contains the IP addresses for the far-end VXLAN Tunnel End Points (VTEPs). The valid range is 1–32 characters. The IP addresses in this list are used to dynamically create service distribution points (SDPs) for the VXLAN service.
mc_group_address	The multicast IP address of the group to which this service will join.
tandem	Specifies the tandem replication mode for the service associated with this UNP. This mode uses PIM routing and sends traffic through multicast SDPs.
headend	Specifies the head-end replication mode for the service associated with this UNP. This mode sends traffic through unicast SDPs.
hybrid	Specifies the hybrid replication mode for the service associated with this UNP. This mode uses both the head-end and tandem methods.
vlan-translation	Configures egress VLAN translation for the VXLAN service associated with this UNP.

Defaults

By default, no mapping configuration is applied to a profile. When the VXLAN mapping is configured, the following default values are applied for the optional parameters:

parameter	default
multicast-mode {headend | tandem | hybrid}	hybrid
vlan-xlation {enable | disable}	disabled

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to disable VLAN translation, remove a far-end IP list, or remove a multicast group IP address for the profile. To remove any other VXLAN mapping parameter requires deleting the entire profile from the switch configuration (**no unp profile** *profile_name*).
- Configuring a new VXLAN mapping for a profile will overwrite the existing VXLAN mapping for that profile.
- Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.
- Only one type of profile mapping (VLAN, SPB, VXLAN, or static) is associated with a profile at any given time.
  - If a profile is mapped to SPB, VXLAN, or static service parameters, then the profile is applied to traffic received on UNP access ports.
  - If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.
- The **tag-value** parameter specifies the VLAN tag values that are used to create the SAP to which profile traffic is mapped. The SAP is then bound to the VXLAN service that is dynamically created based on the specified VXLAN ID value.
- Consider the following when configuring the profile tag value:
  - If the tag value is set to zero, the SAP for the classified traffic is created using the VLAN tags of the traffic. For example, a SAP with an encapsulation value set to 1/12:5 is created when classified traffic received on port 1/12 is single-tagged with VLAN ID 5.
  - Enabling the trust VLAN tag option for the UNP service port triggers the same functionality as setting the service profile tag value to zero. In both cases, the VLAN tags of the classified traffic are used to specify the encapsulation value of the SAP on which the traffic is forwarded.
  - If the trust VLAN tag option is disabled for the UNP port and the service profile tag value is *not* set to zero (for example, **tag-value** 10), the VLAN tag values of the classified traffic are compared to the configured profile tag value. If the traffic tag values match the profile tag value, the traffic is forwarded on the SAP. If the traffic tags do not match, traffic is not forwarded on the SAP.
- UNP first checks the switch configuration to see if a SAP already exists for the expected VLAN tag value (CVLAN tags). If a SAP already exists, the MAC addresses are learned on that SAP. If the SAP does not exist, the switch dynamically creates one based on the profile attributes for the profile traffic.

- If the VXLAN ID specified with this command does not exist in the switch configuration, the switch will dynamically create the expected service and then the SAP as needed.
- Dynamically creating services and related SAPs is subject to available switch resources. If an attempt to dynamically create a service or SAP fails, the MAC addresses classified for the service profile are learned as filtering.
- The same far-end IP list can be used for multiple services that have to reach the same set of far-end VTEPs.
- Configuring both a far-end IP list and a multicast group IP address is allowed for the same profile.
- The following multicast modes are supported for a VXLAN service:
  - **Tandem**: In this mode, PIM multicast routing is required to discover the neighbor nodes and assign membership to VTEP nodes that desire to be in the same multicast group. This also requires the manual configuration of a multicast SDP object to tunnel traffic to the other VTEP nodes that belong to the same multicast group.
  - **Headend**: In this mode, unicast SDP objects are manually configured to tunnel traffic to the far-end nodes. In this case, PIM multicast routing is not required. Any BUM traffic is replicated and one copy is sent to each VTEP node as specified by the unicast SDP object.
  - **Hybrid**: In this mode, traffic is tunneled from this service instance to both a group of VTEPs that belong to the same multicast group address and to the VTEP nodes that are not associated with the same multicast group address.
- Configuring a VXLAN service on an OmniSwitch 6900-V72 or OmniSwitch 6900-C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. If the hybrid mode is selected, only the head-end mode is active.
- Enabling VLAN translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled.

Examples

```
-> unp profile unp1-vxlan map service-type vxlan tag-value 10:12 vnid 100
multicast-group 225.1.1.1
-> unp profile unp2-vxlan map service-type vxlan tag-value 15 vnid 200 far-end-ip-
list vtep-list1 vlan-xlation
-> unp profile unp3-vxlan map service-type vxlan tag-value 0 vnid 200 far-end-ip-
list vtep-list2 multicast-group 225.1.1.2
-> no unp profile unp3-vxlan map service-type vxlan vlan-xlation far-end-ip-list
-> no unp profile unp2-vxlan
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile.
unp profile map vlan	Maps VLAN IDs to a UNP profile. Traffic assigned to the profile is forwarded on the associated VLAN IDs.
unp profile map service-type spb	Maps SPB parameters to a profile. The parameters are used for creating an SPB service access point (SAP) to forward profile traffic.
unp profile map service-type static	Maps an existing SPB or VXLAN service ID to a profile.
unp vxlan far-end-ip-list	Configures a list of IP addresses that represent far-end VXLAN nodes.
show unp profile map	Displays the VLAN or service mapping configuration for the profile.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
alaDaUNPProfileMapVxlanTable
   alaDaUNPProfileMapVxlanEncapVal
   alaDaUNPProfileMapVxlanVnid
   alaDaUNPProfileMapVxlanFarEndIPList
   alaDaUNPProfileMapVxlanMulticastIPAddressType
   alaDaUNPProfileMapVxlanMulticastIPAddress
   alaDaUNPProfileMapVxlanVlanXlation
   alaDaUNPProfileMapVxlanMulticastMode
```

unp vxlan far-end-ip-list

Configures a list of IP addresses, each of which is assigned to the Loopback0 interface of a far-end VXLAN node. The list name is assigned to a profile through the mapping of VXLAN service parameters to the profile. This allows multiple far-end nodes to be associated with the service created for the VXLAN Network ID (VNID) specified in the VXLAN profile.

unp vxlan far-end-ip-list *ip_list_name ip_address* **[***ip_address***]**

no unp vxlan far-end-ip-list *ip_list_name* **[***ip_address* **[***ip_address***]]**

Syntax Definitions

ip_list_name	The name of the list that contains the IP addresses for the far-end VXLAN Tunnel End Points (VTEP). The valid range is 1–32 characters.
ip_address	The IP address of the Loopback0 interface for the far-end VTEP node. The Loopback0 address is required on every VXLAN node that serves as a VTEP. Use a space to specify a list of IP addresses to assign to the list name.

Defaults

N/A

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the far-end list from the switch configuration or to remove an individual IP address from the list.
- The reachability of a far-end IP address is not tested. Make sure the addresses are valid before adding them to the list.
- There is no limit to the number of IP addresses that can be assigned to a single list.
- The same far-end IP list can be used for multiple services that have to reach the same set of far-end VTEPs.
- The far-end IP list is used to build service distribution points (SDPs) for VXLAN services.
- When there is any change to the VXLAN profile, all users associated with that profile are flushed.
- Configuring VXLAN service on an OmniSwitch 6900-V72 or OmniSwitch 6900-C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. If the hybrid mode is selected, only the head-end mode is active.

Examples

```
-> unp vxlan far-end-ip-list vtep-list1 10.1.1.1 11.1.1.1 12.1.1.1 13.1.1.1
-> no unp vxlan far-end-ip-list vtep-list1 10.1.1.1
-> no unp vxlan far-end-ip-list vtep-list1
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp profile	Configures a UNP profile.
unp profile map service-type vxlan	Maps VXLAN parameters, such as a far-end IP list, to a UNP profile.
show unp profile	Displays the profile configuration for the switch.
show unp vxlan far-end-ip-list	Displays the contents of VXLAN far-end IP address lists.

MIB Objects

```
alaDaUNPVxlanFarEndIPAddressListTable
   alaDaUNPVxlanFarEndIPAddressListIPType
   alaDaUNPVxlanFarEndIPAddressListIP
alaDaUNPVxlanFarEndIPListTable
   alaDaUNPVxlanFarEndIPListName
   alaDaUNPVxlanFarEndIPListIPAddressCount
   alaDaUNPVxlanFarEndIPListRemove
```

unp profile map service-type l2gre

Configures the mapping of a Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel to the specified UNP profile. When a device is dynamically assigned to the profile through authentication or classification, an L2 GRE Service Access Point (SAP) is dynamically created using the specified service parameters. Traffic from the device is then encapsulated and forwarded through an L2 GRE tunnel to a tunnel aggregation switch.

unp profile *profile_name* **map service-type l2gre tag-value {0 |** *qtag* | *outer_qtag:inner_qtag***} vpnid** *vpn_id* **{far-end-ip-list** *ip_list_name* **| far-end-ip** *ip_address***} [port-isolation-disable] [vlan-xlation]**

no unp profile *profile_name* **map service-type l2gre [far-end-ip-list | far-end-ip | vlan-xlation]**

Syntax Definitions

profile_name	The name of an existing UNP profile.
0	Use VLAN tag information from classified traffic to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
qtag	The outer VLAN ID tag to use when creating a SAP for single-tagged traffic.
outer_qtag:inner_qtag	An outer VLAN ID tag and an inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
vpn_id	A GRE tunnel Virtual Private Network (VPN) ID. This is a unique value that is used in the header of a GRE encapsulated packet and should be the same at both ends of a Guest Tunnel.
ip_list_name	The name of an existing list that contains the IP address of the Loopback0 interface configured on the far-end tunnel aggregation switch. The valid range is 1–32 characters. The IP address in this list is used to dynamically create the L2 GRE tunnel from the edge switch to the tunnel aggregation switch.
ip_address	The IP address of the Loopback0 interface configured on the far-end tunnel aggregation switch.
vlan-xlation	Configures egress VLAN translation for the service associated with this UNP.

Defaults

By default, no mapping configuration is applied to a profile. When the L2 GRE tunnel service mapping is configured, the following default values are applied for the optional parameters:

parameter	default
vlan-xlation	disabled

Platforms Supported

OmniSwitch 6560, 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- Use the **no** form of this command to do the following;
  - remove a far-end IP list or a far-end IP address for the profile.
  - disable VLAN translation for the dynamic SAP.
- To remove any other L2 GRE mapping parameters requires deleting the entire profile from the switch configuration (**no unp profile** *profile_name*).
- The **tag-value** parameter specifies the VLAN tag values that are used to create the SAP to which profile traffic is mapped. The SAP is then bound to the L2 GRE tunnel that is dynamically created based on the specified VPN ID value.
- The same far-end IP address can be used for multiple L2 GRE tunnels that have to reach the same far-end tunnel aggregation switch.
- Configuring a new L2 GRE tunnel mapping for a profile will overwrite the existing tunnel mapping for that profile.
- Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.
- Only one type of profile mapping (VLAN, SPB, VXLAN, L2 GRE tunnel, or static) is associated with a profile at any given time.
- A UNP L2 GRE profile is applied to users learned on UNP bridge and access ports.
  - Classifying users learned on UNP bridge ports into an L2 GRE profile is supported on the OmniSwitch 6560, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, 6900-X72, and OmniSwitch 9900.
  - Classifying users learned on UNP access ports into an L2 GRE profile is supported on the OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900-Q32, 6900-X72, and OmniSwitch 9900.
  - Only one UNP L2 GRE profile (one L2 GRE service) can be applied to users learned on UNP bridge ports. The exception to this is on an OmniSwitch 6560 where up to eight UNP L2 GRE profiles (eight L2 GRE services) can be applied to users learned on UNP bridge ports.
  - Multiple UNP L2 GRE profiles (multiple L2 GRE services) can be applied to users learned on UNP access ports.
  - When users are learned on UNP bridge ports and classified into an L2 GRE profile, the VLAN translation status is not applied. VLAN translation only applies to user traffic learned on UNP access ports.
  - The mobile tag functionality is supported on UNP L2 GRE profiles and is applied when users learned on UNP access ports are dynamically assigned to the profile; this functionality is not supported for users learned on UNP bridge ports. Use the **unp profile mobile-tag** command to configure the mobile tag status for the profile.
  - There is no VLAN association with the SAP created for the L2 GRE tunnel, so all traffic egressing on the UNP bridge port will be untagged.
- UNP first checks the switch configuration to see if an L2 GRE tunnel SAP already exists for the expected VPN ID. If a SAP already exists, the MAC addresses are learned on that SAP. If the SAP does not exist, the switch dynamically creates one based on the profile attributes for the profile traffic.
- If the GRE tunnel VPN ID specified with this command does not exist in the switch configuration, the switch will dynamically create the expected service and then the SAP as needed.
- Dynamically creating services and related SAPs is subject to available switch resources. If an attempt to dynamically create a service or SAP fails, the MAC addresses classified for the UNP GRE tunnel profile are learned as filtering.

Examples

```
-> unp profile guest-profile map service-type l2gre tag-value 0 vpnid 100 far-end-
ip 192.168.10.1
-> unp profile guest-profile map service-type l2gre tag-value 0 vpnid 100 far-end-
ip-list l2greEndpoint
-> unp profile guest-profile map service-type l2gre tag-value 0 vpnid 200 far-end-
ip 192.168.10.1 vlan-xlation
-> no unp profile guest-profile map service-type l2gre far-end-ip-list
-> no unp profile guest-profile map service-type l2gre vlan-xlation
-> no unp profile guest-profile map service-type l2gre
-> no unp profile guest-profile
```

Release History

Release 8.4.1.R02; command was introduced.
Release 8.6R1; **vlan-xlation** parameter added.

Related Commands

unp profile	Configures a UNP profile.
unp profile mobile-tag	Configures the mobile tag status for the specified profile.
unp l2gre far-end-ip-list	Configures a list of IP addresses that represent far-end Guest Tunnel Termination Switch.
show unp profile map	Displays the VLAN or service mapping configuration for the profile.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
alaDaUNPProfileMapL2GreTable
   alaDaUNPProfileMapL2GreEncapVal
   alaDaUNPProfileMapL2GreVpnid
   alaDaUNPProfileMapL2GreFarEndIPAddressType
   alaDaUNPProfileMapL2GreFarEndIPAddress
   alaDaUNPProfileMapL2GreFarEndIPList
   alaDaUNPProfileMapL2GreRowStatus
   alaDaUNPProfileMapL2GreVlanXlation
```

unp l2gre far-end-ip-list

Configures an IP address list that contains the IP address of the Loopback0 interface configured on the far-end L2 GRE tunnel aggregation switch. The list name is assigned to a profile through the mapping of L2 GRE tunnel parameters to the profile.

unp l2gre far-end-ip-list *ip_list_name ip_address*

no unp l2gre far-end-ip-list *ip_list_name* **[***ip_address***]**

Syntax Definitions

ip_list_name	The name of the list that contains the IP address for the far-end tunnel aggregation switch. The valid range is 1–32 characters.
ip_address	The IP address of the Loopback0 interface for the far-end tunnel aggregation switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

- Use the **no** form of this command to remove the far-end list from the switch configuration or to remove the IP address from the list.
- Only one IP address can be assigned to a single list.
- The reachability of a far-end IP address is not tested. Make sure the IP address is valid before adding the address to the list.
- The same far-end IP list can be used on multiple L2 GRE tunnel access switches that have to reach the same tunnel aggregation switch.
- The far-end IP list is used to build L2 GRE tunnels to the tunnel aggregation switch.
- When there is any change to the L2 GRE profile associated with the far-end IP list, all users associated with that profile are flushed.

Examples

```
-> unp l2gre far-end-ip-list l2gre-ip-list 192.168.10.1
-> no unp l2gre far-end-ip-list l2gre-ip-list 192.168.10.1
-> no unp l2gre far-end-ip-list l2gre-ip-list
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

unp profile	Configures a UNP profile.
unp profile map service-type l2gre	Maps L2 GRE tunnel parameters, such as a far-end IP list, to a UNP profile.
show unp profile	Displays the profile configuration for the switch.
show unp l2gre far-end-ip-list	Displays the contents of a far-end IP address list for an L2 GRE tunnel.

MIB Objects

```
alaDaUNPL2GreFarEndIPAddressListTable
   alaDaUNPL2GreFarEndIPAddressListIPType
   alaDaUNPL2GreFarEndIPAddressListIP
   alaDaUNPL2GreFarEndIPAddressListRowStatus
alaDaUNPL2GreFarEndIPListTable
   alaDaUNPL2GreFarEndIPListName
   alaDaUNPL2GreFarEndIPListIPAddressCount
   alaDaUNPL2GreFarEndIPListRemove
```

unp profile map service-type static

Configures the mapping of an existing Shortest Path Bridging (SPB) or Virtual eXtensible LAN (VXLAN) service ID to the specified UNP profile. This type of profile mapping is only valid if the specified SPB or VXLAN service is already configured; the switch does not dynamically create the service. The specified service ID is then used to dynamically create a service access point (SAP) based on the specified tag value.

unp profile *profile_name* **map service-type static tag-value {0 |** *qtag* | *outer_qtag:inner_qtag}* **service-id** *service_id*

Syntax Definitions

profile_name	The name of an existing UNP profile.
0	Use VLAN tag information from classified traffic to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
qtag	The outer VLAN ID tag to use when creating a SAP for single-tagged traffic.
outer_qtag:inner_qtag	An outer VLAN ID tag and an inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
service_id	An existing (statically configured) numerical value that identifies a specific SPB or VXLAN service. The valid service ID range is 1–32767. *Specifying a VXLAN service ID is supported only on the OmniSwitch 6900-V72, OmniSwitch 6900-C32, OmniSwitch 6900-Q32, and OmniSwitch 6900-X72.*

Defaults

By default, no mapping configuration is applied to a profile.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Removing a static service mapping configuration requires deleting the entire profile from the switch configuration (**no unp profile** *profile_name*).
- Configuring a new static service mapping for a profile will overwrite the existing static service mapping for that profile.
- Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.
- Only one type of profile mapping (VLAN, SPB, VXLAN, or static) is associated with a profile at any given time.
- If a profile is mapped to SPB, VXLAN, or static service parameters, then the profile is applied to traffic received on UNP access ports.

- If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.
- The **tag-value** parameter specifies the VLAN tag values that are used to create the SAP to which profile traffic is mapped. The SAP is then bound to the service ID value specified with this command.
- Consider the following when configuring the profile tag value:
  - If the tag value is set to zero, the SAP for the classified traffic is created using the VLAN tags of the traffic. For example, a SAP with an encapsulation value set to 1/12:5 is created when classified traffic received on port 1/12 is single-tagged with VLAN ID 5.
  - Enabling the trust VLAN tag option for the UNP service port triggers the same functionality as setting the service profile tag value to zero. In both cases, the VLAN tags of the classified traffic are used to specify the encapsulation value of the SAP to which the traffic is mapped.
  - If the trust VLAN tag option is disabled for the UNP port and the service profile tag value is *not* set to zero (for example, **tag-value** 10), the VLAN tag values of the classified traffic are compared to the configured profile tag value. If the traffic tag values match the profile tag value, the traffic is mapped to the appropriate SAP. If the traffic tags do not match, traffic is not mapped to a SAP.
- UNP first checks the switch configuration to see if a SAP already exists for the expected VLAN tag value (CVLAN tags) and service ID. If a SAP already exists, the MAC addresses are learned on that SAP. If the SAP does not exist, the switch dynamically creates one for the profile traffic.
- When there is a MAC flush for all UNP users learned and forwarded on the static service ID:
  - UNP triggers the removal of all dynamic SAPs associated with the service ID.
  - The service ID is not removed because the service was statically created; not dynamically generated through UNP.
- A static service ID cannot be removed until all the UNP users learned and forwarded on that service and associated SAPs are deleted.

Examples

```
-> unp profile unp1-static map service-type static tag-value 10 service-id 1
-> unp profile unp2-static map service-type static tag-value 20 service-id 2
-> no unp profile unp1-static
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile.
unp profile map vlan	Maps VLAN IDs to a UNP profile. Traffic assigned to the profile is forwarded on the associated VLAN IDs.
unp profile map service-type spb	Maps SPB parameters to a profile. The parameters are used for creating an SPB service access point (SAP) to forward profile traffic.
unp profile map service-type vxlan	Maps VXLAN parameters to a profile. The parameters are used for creating a VXLAN service access point (SAP) to forward profile traffic.
show unp profile map	Displays the VLAN or service mapping configuration for the profile.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
alaDaUNPProfileMapStaticTable
   alaDaUNPProfileMapStaticEncapVal
   alaDaUNPProfileMapStaticServiceID
```

unp system-default service-mod

Specifies the modulo number that the switch will use to dynamically calculate an SPB Service Instance Identifier (I-SID) value or a VXLAN Network Identifier (VNID) value for a System Default profile. System Default profiles are dynamically created to accommodate device traffic received on UNP access ports that is not classified into a user-defined UNP service profile.

unp system-default service-mod {*mod_number* **| default}**

Syntax Definitions

mod_number	The modulo number to use for calculating an SPB I-SID or VNID value. The valid range is 1–4096.
default	Sets the modulo number value back to the default value.

Defaults

By default, modulo 512 is used for the System Default profile calculation.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A System Default profile is defined to carry traffic for an SPB service or for a VXLAN service based on the dynamic service setting for the UNP access port on which the traffic is received (see the **unp dynamic-service** command**)**. For example:
  - If the dynamic service value is set to SPB, then the System Default profile is dynamically created with attributes to define an SPB SAP.
  - If the dynamic service value is set to VXLAN, then the System Default profile is dynamically created with attributes to define a VXLAN SAP.
- One of the attributes defined for a System Default profile is an SPB I-SID or VXLAN VNID. This value is dynamically calculated using the base service number, modulo number, VLAN tag of the UNP port traffic, and the UNP port domain value. For example, if the base service number is 10000000, the modulo number is 512, the VLAN tag is 30, and the domain is 10, then the following calculation is used to determine the SPB I-SID or VXLAN VNID number:

  10000000 + (10 * 10000) + (30 % 512) = 10100030

  Based on the above calculation, “10100030” is the resulting service instance value.
- Once the SPB I-SID or VXLAN VNID number is determined, that number is used to derive the System Default profile name. For example:
  - The name of an SPB System Default profile is “SystemDefaultISID”, where ISID is the calculated attribute value for the profile. For example, if the calculated I-SID number is 10100030, then the SPB profile “SystemDefault10100030” is created.
  - The name of a VXLAN System Default profile is “SystemDefaultVNID”, where VNID is the calculated attribute value for the profile. For example, if the calculated VNID number is 10000100, then the VXLAN profile “SystemDefault10001000” is created.

- When the modulo number value is changed, all users learned in System Default profiles are flushed (logged out of the network) and dynamic SAPs created for the profiles are cleared.

Examples

```
-> unp system-default service-mod 800
-> unp system-default service-mod default
```

Release History

Release 8.5R1; command was introduced.

Related Commands

unp system-default service-base	Specifies the base service number that the switch will use to dynamically calculate an SPB I-SID value or a VXLAN VNID value for a System Default profile.
unp system-default multicastmode	Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.
unp system-default vlan-xlation	Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.
unp system-default multicastgroup	Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.
unp system-default far-end-ip-list	Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.
show unp global configuration	Displays the configurable System Default profile values for the switch.
unp dynamic-service	Configures whether the System Default service profile dynamically creates an SPB SAP or a VXLAN SAP based on the traffic received on the UNP access port.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPServiceModule
```

unp system-default service-base

Specifies the base service number that the switch will use to dynamically calculate an SPB Service Instance Identifier (I-SID) value or a VXLAN Network Identifier (VNID) value for a System Default profile. System Default profiles are dynamically created to accommodate device traffic received on UNP access ports that is not classified into a user-defined UNP service profile.

unp system-default service-base {*base_number* **| default}**

Syntax Definitions

base_number	The base service number to use for calculating an SPB I-SID or VNID value. The valid range is 1–10000000.
default	Sets the base service number value back to the default value.

Defaults

By default, base service number 10,000,000 is used for the System Default profile calculation.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- A System Default profile is defined to carry traffic for an SPB service or for a VXLAN service based on the dynamic service setting for the UNP access port on which the traffic is received (see the **unp dynamic-service** command**)**. For example:
  - If the dynamic service value is set to SPB, then the System Default profile is dynamically created with attributes to define an SPB SAP.
  - If the dynamic service value is set to VXLAN, then the System Default profile is dynamically created with attributes to define a VXLAN SAP.
- One of the attributes defined for a System Default profile is an SPB I-SID or VXLAN VNID. This value is dynamically calculated using the base service number, modulo number, VLAN tag of the UNP port traffic, and the UNP port domain value. For example, if the base service number is 10,000,000, the modulo number is 512, the VLAN tag is 30, and the domain is 10, then the following calculation is used to determine the SPB I-SID or VXLAN VNID number:

  10,000,000 + (10 * 10,000) + (30 % 512) = 10,100,030

  Based on the above calculation, “10,100,030” is the resulting service instance value.
- Once the SPB I-SID or VXLAN VNID number is determined, that number is used to derive the System Default profile name. For example:
  - The name of an SPB System Default profile is “SystemDefaultISID”, where ISID is the calculated attribute value for the profile. For example, if the calculated I-SID number is “10,100,030”, then the SPB profile “SystemDefault10100030” is created.
  - The name of a VXLAN System Default profile is “SystemDefaultVNID”, where VNID is the calculated attribute value for the profile. For example, if the calculated VNID number is “10,001,000”, then the VXLAN profile “SystemDefault10001000” is created.

- When the base service number value is changed, subsequent System Default profiles are created with the new value while profiles created with the previous base value are retained.

Examples

```
-> unp system-default service-base 5000
-> unp system-default service-base default
```

Release History

Release 8.5R1; command was introduced.

Related Commands

unp system-default service-mod	Specifies the modulo number that the switch will use to dynamically calculate an SPB I-SID value or a VXLAN VNID value for a System Default profile.
unp system-default multicastmode	Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.
unp system-default vlan-xlation	Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.
unp system-default multicastgroup	Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.
unp system-default far-end-ip-list	Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.
show unp global configuration	Displays the configurable System Default profile values for the switch.
unp dynamic-service	Configures whether the System Default service profile dynamically creates an SPB SAP or a VXLAN SAP based on the traffic received on the UNP access port.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPServiceBase
```

unp system-default multicastmode

Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.

unp system-default multicastmode {tandem | headend | hybrid}

Syntax Definitions

tandem	Specifies the tandem replication mode for services dynamically created for System Default profiles.
headend	Specifies the head-end replication mode for services dynamically created for System Default profiles.
hybrid	Specifies the hybrid replication mode for services dynamically created for System Default profiles.

Defaults

By default, System Default profile services are configured to use the head-end mode.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The multicast mode selection specified with this command is a global setting that is applied to all of the dynamic services that are created for System Default profiles.
- The following multicast modes are supported for an SPB service:
  - **Tandem**: In this mode, a non-unicast packet received on an SPB access port is replicated once at each node using the multicast group address.
  - **Headend**: In this mode, a non-unicast packet received on an SPB access port is replicated once for each receiver in the provider backbone bridge (PBB) network using its unicast base MAC (BMAC) address.
- The following multicast modes are supported for a VXLAN service:
  - **Tandem**: In this mode, PIM multicast routing is required to discover the neighbor nodes and assign membership to VTEP nodes that desire to be in the same multicast group. This also requires the manual configuration of a multicast SDP object to tunnel traffic to the other VTEP nodes that belong to the same multicast group.
  - **Headend**: In this mode, unicast SDP objects are manually configured to tunnel traffic to the far-end nodes. In this case, PIM multicast routing is not required. Any BUM traffic is replicated and one copy is sent to each VTEP node as specified by the unicast SDP object.
  - **Hybrid**: In this mode, traffic is tunneled from this service instance to both a group of VTEPs that belong to the same multicast group address and to the VTEP nodes that are not associated with the same multicast group address.

Examples

```
-> unp system-default multicastmode tandem
-> unp system-default multicastmode headend
```

```
-> unp system-default multicastmode hybrid
```

Release History

Release 8.5R1; command was introduced.
Release 8.6R2; **hybrid** parameter added.

Related Commands

unp system-default vlan-xlation	Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.
unp system-default multicastgroup	Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.
unp system-default far-end-ip-list	Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.
show unp global configuration	Displays the configurable System Default profile values for the switch.
show unp profile map	Displays the VLAN or service mapping configuration for the profile.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPServiceMulticastMode
```

unp system-default vlan-xlation

Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.

unp system-default vlan-translation {enable | disable}

Syntax Definitions

enable	Enables egress translation of VLAN tags.
disable	Disables egress translation of VLAN tags.

Defaults

By default, VLAN translation is enabled for System Default profile services.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- The VLAN translation status specified with this command is a global setting that is applied to all of the dynamic services that are created for System Default profiles.
- When VLAN translation is enabled for a service, the VLAN tags for outgoing frames on SAPs associated with that service are processed according to the local SAP configuration (the SAP on which the frames will egress) and not according to the configuration of the SAP on which the frames were received.
- When VLAN translation is disabled, frames simply egress without any modification of the VLAN tags. In other words, the frames are transparently bridged without tag modification.

Examples

```
-> unp system-default vlan-xlation disable
-> unp system-default vlan-xlation enable
```

Release History

Release 8.5R1; command was introduced.

Related Commands

unp system-default multicastmode	Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.
unp system-default multicastgroup	Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.
unp system-default far-end-ip-list	Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.
show unp global configuration	Displays the configurable System Default profile values for the switch.
show unp profile map	Displays the VLAN or service mapping configuration for the profile.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPServiceVlanXlation
```

unp system-default multicastgroup

Specifies a multicast group IP address to associate with dynamic VXLAN services that are created for System Default profiles.

unp system-default multicastgroup {*mc_group_address* | **default}**

Syntax Definitions

mc_group_address	The multicast IP address of the group to which this service will join.
default	Sets the multicast group IP address back to the default value (239.0.0.0).

Defaults

By default, a VXLAN service associated with a System Default profile will join the 239.0.0.0 multicast group.

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- The multicast group IP address specified with this command is a global setting that is applied to all of the dynamic VXLAN services that are created for System Default profiles.
- When a dynamic VXLAN service is created for a System Default profile, the specified multicast group IP address is used to build a VXLAN Service Distribution Point (SDP) tunnel for the VXLAN service traffic. VXLAN nodes that subscribe to the same multicast group will receive traffic through the associated SDP tunnel from all the other VXLAN nodes that belong to the same multicast group.

Examples

```
-> unp system-default multicastgroup 225.1.1.2
-> unp system-default multicastgroup 239.0.0.0
-> unp system-default multicastgroup default
```

Release History

Release 8.5R1; command was introduced.

Related Commands

unp system-default multicastmode	Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.
unp system-default vlan-xlation	Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.
unp system-default far-end-ip-list	Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.
show unp global configuration	Displays the configurable System Default profile values for the switch.
show unp profile map	Displays the VLAN or service mapping configuration for the profile.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPServiceMulticastGroup
```

unp system-default far-end-ip-list

Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles. The list contains IP addresses assigned to the Loopback0 interfaces of far-end VXLAN nodes. This allows multiple far-end nodes to be associated with the dynamic service created for the VXLAN Network ID (VNID) specified in a VXLAN System Default profile.

unp system-default far-end-ip-list {*ip_list_name* | **default}**

Syntax Definitions

ip_list_name	The name of the list that contains the IP addresses for the far-end VXLAN Tunnel End Point (VTEP) nodes. The valid range is 1–32 characters.
default	Sets the far-end list name to the default value (no list name is specified).

Defaults

N/A

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- The far-end IP list name specified with this command is a global setting that is applied to all of the dynamic VXLAN services that are created for System Default profiles.
- When a dynamic VXLAN service is created for a System Default profile, the specified IP address list name is used to build VXLAN Service Distribution Point (SDP) tunnels between the VXLAN nodes. Traffic associated with the dynamic VXLAN service is encapsulated and sent through an SDP tunnel to the destined far-end node.

Examples

```
-> unp system-default far-end-ip-list vtep-list1
-> unp system-default far-end-ip-list default
```

Release History

Release 8.5R1; command was introduced.
Release 8.6R2; **default** parameter added.

Related Commands

unp system-default multicastmode	Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.
unp system-default vlan-xlation	Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.
unp system-default multicastgroup	Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.
show unp global configuration	Displays the configurable System Default profile values for the switch.
show unp profile map	Displays the VLAN or service mapping configuration for the profile.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPServiceFarEndIpList
```

unp saa-profile

Configures a Service Assurance Agent (SAA) performance monitoring profile. This type of profile is assigned to UNP profiles to specify jitter and latency threshold values for SAA sessions that apply to the assigned UNP profile.

unp saa-profile *profile_name* **[jitter-threshold** *jitter_thresh***] [latency-threshold** *latency_thresh***]**

no unp saa-profile *profile_name*

Syntax Definitions

profile_name	The name to assign to the SAA profile.
jitter_thresh	The jitter threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.
latency_thresh	The latency threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.

Defaults

parameter	default
jitter_thresh	0 (disabled)
latency_thresh	0 (disabled)

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the SAA profile from the switch configuration.
- Although SAA profiles can be configured and assigned to a UNP through the CLI, these profiles are mainly used by the OmniVista network management application to trigger SAA sessions that monitor connections between virtual machines (VMs) in a data center network.
- Assigning SAA profiles is supported only with UNP profiles that are assigned to UNP bridge ports. UNP access ports do not support this functionality.

Examples

```
-> unp saa-profile unp_saa1 jitter-threshold 100 latency-threshold 500
-> unp saa-profile unp_saa2 jitter-threshold 150
-> unp saa-profile unp_saa3 latency-threshold 250
```

Release History

Release 7.3.2; command was introduced.

Related Commands

unp profile saa-profile	Assigns an SAA profile to the specified UNP profile.
show unp saa-profile	Displays the SAA profile configuration for the switch.
show unp profile	Displays the profile configuration for the switch.

MIB Objects

```
alaDaSaaProfileTable
   alaDaSaaProfileName
   alaDaSaaProfileLatencyThreshold
   alaDaSaaProfileJitterThreshold
```

unp port-type

Configures UNP functionality for the specified port or link aggregate. This includes configuring the UNP port type (bridge or access). Traffic received on a UNP bridge port is classified using VLAN profiles and port attributes. Traffic received on a UNP access port is classified using service profiles and port attributes.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id1***[-***agg_id2***]} port-type {access | bridge}**

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id1***[-***agg_id2***]}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port1***[-***port***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id1***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (5-10).
access	Configures the specified port or link aggregate as a service access port. This port type is used for classifying traffic into service-based profiles. T*his parameter is not supported on the OmniSwitch 6465 or OmniSwitch 6560.*
bridge	Configures the specified port or link aggregate as a standard bridge port. This port type is used for classifying traffic into VLAN-based profiles.

Defaults

By default, UNP is disabled on all ports and link aggregates.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the UNP configuration from a port or link aggregate.
- Any configuration change to a UNP-enabled port will flush all MAC addresses learned on that port. This applies only to CLI commands used to configure UNP port parameters.
- Only one UNP port type is configurable for a specific port or link aggregate. To change the port type of an existing UNP port, remove the current UNP configuration first using the **no unp port** or **no unp linkagg** command then use the **unp port-type** command to set the new port type.
- There is no limit to the number of switch ports that can have UNP enabled.
- Enabling UNP is *not* supported on the following switch ports:
  - 802.1q-tagged ports.
  - MVRP ports.
  - Port Mirroring destination ports (MTP).

  - Port Mapping network ports.
  - STP and ERP ports.
  - Ports on which a static MAC address is configured.
  - Ports on which dynamic Source Learning is disabled.
  - VLAN Stacking (Ethernet Services NNI or UNI) ports.
  - Service Manager access and network ports.
  - Ethernet OAM ports.

- UNP and Learned Port Security (LPS) are supported on the same port with the following conditions:
  - LPS is not supported on link aggregates.
  - The LPS learning window is set globally but not on a per-port basis. So the window applies to all UNP ports.
  - When LPS is enabled or disabled on a UNP bridge port (LPS is not supported on UNP access ports), MAC addresses already learned on that port are flushed.
  - Configuring a static MAC address is not allowed on a UNP port unless LPS is also enabled on the same port.
  - When both LPS and UNP are enabled on the same port, UNP first authenticates and classifies any MAC addresses received, then LPS rules are applied. If a MAC address violates any of the LPS rules for the port, the address may get filtered or the port violated even if UNP initially determined the address was valid. In other words, LPS rules take precedence over UNP to determine if a MAC address is bridged or filtered on the port.
  - If UNP classifies a MAC address as learning but LPS learns the address as filtering, an untagged packet will show as filtering in the default VLAN for the port and a tagged packet MAC will show as filtering in the specific tagged VLAN.
  - When a MAC address is filtered by LPS, the **show unp user** command will display “LPS-Blocked” as the classification source for that MAC address.

- UNP ports support both tagged and untagged packets. If the VLAN ID of a tagged packet matches the VLAN associated with a UNP into which the packet was classified, the packet is learned as forwarding and a tagged VLAN-port association is created. However, if the VLAN ID tag does not match the VLAN ID associated with the profile, the packet is filtered.

- UNP bridge and access ports support single-tagged and double-tagged packets with the following conditions:
  - Double-tagged packets are treated the same as single-tagged packets in that UNP will only use the outer VLAN tag to determine how the packet is processed on the UNP bridge port.
  - UNP access ports use the inner VLAN tag of double-tagged packets received on the port to determine the service access port (SAP) to use or create for forwarding the traffic on the network backbone.

Examples

```
-> unp port 1/1 port-type access
-> unp port 1/1-3 port-type bridge
-> unp port 1/10 port-type access
-> no unp port 1/10
-> unp linkagg 5 port-type access
-> unp linkagg 8 port-type bridge
-> unp linkagg 2 port-type access
-> no unp linkagg 2
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp admin-state	Configures the administrative status of the UNP configuration for the specified port or link aggregate.
unp profile	Configures a UNP profile that is used to classify traffic received on UNP ports.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortType
```

unp l2-profile

Assigns an existing Layer 2 profile to the specified UNP access port. This profile determines how Layer 2 protocol frames received on the access port are processed.

unp {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} l2-profile** *l2profile_name*

no unp {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} l2-profile**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
l2profile_name	The name of an existing Layer 2 profile.

Defaults

By default, the Layer 2 profile “unp-def-access-profile” is assigned when a port is configured as a UNP access port.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the Layer 2 profile configuration from the UNP port.
- Specify only ports or link aggregates that are configured as UNP access ports. This command does not apply to UNP bridge ports.
- Specify a Layer 2 profile name that already exists in the switch configuration. Layer 2 profiles are created using the **service l2profile** command.

Examples

```
-> unp port 1/1/3 l2-profile sap_1_profile
-> unp linkagg 10 l2-profile sap_1_profile
-> unp port 1/1/3 l2-profile unp-def-access-profile
-> unp linkagg 10 l2-profile unp-def-access-profile
-> no unp port 1/1/3 l2-profile
-> no unp linkagg 10 l2-profile
```

Release History

Release 8.4.1; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
service l2profile	Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.
show service l2profile	Displays the Layer 2 profile configuration information for the bridge.
show unp port config	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortL2Profile
```

unp redirect port-bounce

Enables or disables the port bounce action on the specified UNP bridge port or globally on all UNP bridge ports. When enabled, a port bounce is triggered upon receipt of a RADIUS Change of Authorization (COA) or a Disconnect request (DM) message from a redirection server to enforce a user role or terminate a user session.

unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} redirect port-bounce**

no unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} redirect port-bounce**

unp redirect port-bounce {enable | disable}

Syntax Definitions

*chassis/slot/port***[**-*port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP bridge port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number for a specific UNP bridge link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).
enable	Globally enables the port bounce function for all UNP bridge ports.
disable	Globally disables the port bounce function for all UNP bridge ports.

Defaults

By default, port bounce is disabled on all UNP bridge ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **port** or **linkagg** parameter to enable port bounce for a specific UNP bridge port or link aggregate. Use the **no** form of this command to disable port bounce for a specific UNP bridge port or link aggregate. Note that port bounce is not supported on UNP access ports.
- Use the **enable** or **disable** parameters to globally enable or disable the port bounce status for all UNP bridge ports or link aggregates on the entire switch.
- This command applies only to ports and link aggregates configured as UNP bridge ports; this command does not apply to UNP access ports.
- The port bounce action only applies to a MAC authenticated non-supplicant (non-802.1X device). If the device is a supplicant (802.1X device), then an EAP-Fail frame is sent instead. In both cases, re-authentication is triggered for both types of devices.
- The port-level setting of the port bounce action overrides the global setting for the switch. The following table indicates when a port is toggled based on the status of port bounce at the global and port level:

Global Port Bounce	Per-Port Bounce	Action
Enabled	Disabled	Port is not toggled
Enabled	Enabled	Port is toggled
Disabled	Enabled	Port is toggled
Disabled	Disabled	Port is not toggled

- This command is used when configuring the switch to interact with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch Bring Your Own Devices (BYOD) solution.

Examples

Port-level configuration example:

```
-> unp port 1/1/6 redirect port-bounce
-> no unp port 1/1/6 redirect port-bounce
```

Global configuration example:

```
-> unp redirect port-bounce enable
-> unp redirect port-bounce disable
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; **no** form of this command added for specific port or link aggregate configuration.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp redirect pause-timer	Configures the global pause timer value for the switch
unp redirect proxy-server-port	Configures the HTTP proxy port number to use for redirection.
unp redirect-server	Configures an IP network address to allow HTTP traffic redirection.
unp redirect allowed-name	Configures a list of additional IP addresses to which a host can access.
show unp port	Displays the UNP configuration for the port.
show unp global configuration	Displays the profile designated as the authentication server down UNP for the switch.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortRedirectPortBounce
alaDaUNPGlobalConfiguration
   alaDaUNPRedirectPortBounce
```

unp 802.1x-authentication

Configures the status of 802.1X authentication for the specified UNP port. Enable this functionality to invoke 802.1X-based authentication for devices connected to the UNP port.

unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} 802.1x-authentication**

no unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} 802.1x-authentication**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

By default, 802.1X authentication is enabled on UNP ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable 802.1X authentication on a UNP port or link aggregate.
- This command is only allowed on UNP-enabled ports and link aggregates.
- If a range of ports or link aggregates is specified with this command, any non-UNP ports or aggregates within the range are skipped.
- An option exists to classify a device into an alternate UNP in the event successful 802.1X authentication does not return a UNP name. See the **unp 802.1x-authentication pass-alternate** command.
- If UNP MAC authentication, 802.1X authentication, and classification (see **unp classification** and **unp mac-authentication**) are disabled on the UNP port, all MAC addresses received on that port are blocked unless a default UNP is configured.
- Configuring an authentication server down UNP (see **unp auth-server-down)** is highly recommended when MAC or 802.1X authentication is enabled on VLAN bridge or SPB access ports or aggregates. This is because after a switch reload, traffic from devices connected to these types of ports and aggregates reaches the switch and triggers the authentication process before route convergence has completed and the server can be reached.
  - If an authentication server down UNP is configured, devices are temporarily learned in that profile and authentication is automatically attempted again after the timeout period expires. This allows time for the server to become reachable from the switch after a reload.
  - If an authentication server down UNP is not configured, devices are learned as filtering and will remain in that state. There is no further attempt to authenticate these devices again.

– The authentication server down functionality is *not* supported on VXLAN access ports or aggregates.

Examples

```
-> unp port 1/1/5 802.1x-authentication
-> no unp port 1/1/5 802.1x-authentication

-> unp port 1/1/10-15 802.1x-authentication
-> no unp port 1/1/10-15 802.1x-authentication

-> unp linkagg 10 802.1x-authentication
-> no unp linkagg 20 802.1x-authentication

-> unp linkagg 10-50 802.1x-authentication
-> no unp linkagg 10-50 802.1x-authentication
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication pass-alternate	Assigns the device to another profile when successful 802.1X authentication does not return a UNP name.
unp mac-authentication	Configures the MAC authentication status for the UNP port.
unp classification	Configures the classification status for the UNP port.
unp auth-server-down	Configures an authentication server down UNP for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPort8021XAuthStatus
```

unp 802.1x-authentication pass-alternate

Configures the name of an existing UNP to use as an alternate profile. A device is assigned to the alternate profile when successful 802.1X authentication does not return the name of a profile.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication pass-alternate** *profile_name*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***} 802.1X-authentication pass-alternate**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
profile_name	The name of an existing VLAN, SPB, or VXLAN profile.

Defaults

By default, no alternate UNP is configured.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the alternate profile from the UNP port configuration.
- This command is only allowed on UNP-enabled ports and link aggregates.
- If a range of ports or link aggregates is specified with this command, any non-UNP ports or aggregates within the range are skipped.
- The profile name specified with this command must already exist in the switch configuration.

Examples

```
-> unp port 1/1/1 802.1x-authentication pass-alternate Finance
-> unp port 1/1/1-3 802.1x-authentication pass-alternate CustomerA
-> no unp port 1/1/1-3 802.1x-authentication pass-alternate

-> unp linkagg 5 802.1x-authentication pass-alternate AltUNP
-> unp linkagg 10-15 802.1x-authentication pass-alternate CustomerB
-> no linkagg 5 mac-authentication pass-alternate
```

Release History

Release 7.3.4; command was introduced.
Release 8.3.1; **vlan-profile**, **spb-profile**, and **vxlan-profile** parameters deprecated.

Related Commands

unp profile	Configures a UNP profile that is used to classify traffic received on UNP ports.
unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication	Configures the 802.1X authentication status for the UNP port.
show unp port	Displays the UNP port parameter configuration.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPort8021XPassAltProfileName
```

unp 802.1x-authentication tx-period

Configures the 802.1X authentication re-transmission time interval for the specified UNP port.

unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} 802.1x-authentication tx-period** *seconds*

no unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} 802.1x-authentication tx-period**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
seconds	The amount of time before an EAP Request Identity is retransmitted. The valid range is 1–60 seconds.

Defaults

By default, the retransmission period is set to 30 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to set the re-transmission time interval back to the default value of 30 seconds.
- The re-transmission time period only applies to UNP ports on which 802.1X authentication is enabled.
- If a range of ports is specified with this command, any non-UNP ports within the range are skipped.

Examples

```
-> unp port 1/1/5 802.1x-authentication tx-period 60
-> unp port 1/1/6-10 802.1x-authentication tx-period 20
-> no unp port 1/1/5 802.1x-authentication tx-period

-> unp linkagg 10 802.1x-authentication tx-period 60
-> unp linkagg 20-25 802.1x-authentication tx-period 20
-> no unp linkagg 10 802.1x-authentication tx-period
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication	Configures the 802.1X authentication status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPort8021XTxPeriod
```

unp 802.1x-authentication supp-timeout

Configures the 802.1X authentication supplicant timeout for the specified UNP port. This value is the amount of time the switch will wait before timing out an 802.1X user that is attempting to authenticate.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication supp-timeout** *seconds*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication supp-timeout**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15)
seconds	The timeout value. The valid range is 1–120 seconds.

Defaults

By default, the supplicant timeout value is set to 30 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to set the supplicant timeout back to the default value of 30 seconds.
- Increase the supplicant timeout value if the authentication process requires additional steps by the user (for example, entering a challenge).
- The supplicant timeout is applied only to 802.1X users connected to a UNP port on which 802.1X authentication is enabled.
- If a range of ports is specified with this command, any non-UNP ports within the range are skipped.

Examples

```
-> unp port 1/1/5 802.1x-authentication supp-timeout 10
-> unp port 1/1/10-15 802.1x-authentication supp-timeout 60
-> no unp port 1/1/5 802.1x-authentication supp-timeout

-> unp linkagg 10 802.1x-authentication supp-timeout 40
-> unp linkagg 2-5 802.1x-authentication supp-timeout 40
-> no unp linkagg 10 802.1x-authentication supp-timeout
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication	Configures the 802.1X authentication status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPort8021XSuppTimeOut
```

unp 802.1x-authentication max-req

Configures the maximum number of times the switch will retransmit a request for authentication information (request identity, password, challenge) to an 802.1X user on the specified UNP port.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication max-req** *max_req*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication max-req**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
max_req	The maximum number of times information requests are retransmitted. The valid range is 1–3.

Defaults

By default, the maximum number of requests is set to two.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to set the maximum number of times information requests are retransmitted back to the default value of two.
- The 802.1X requests are transmitted, up to the maximum number allowed, until the authentication session is shut down based on the supplicant timeout value configured for the 802.1X port.
- The maximum number of requests is applied only to 802.1X users connected to a UNP port on which 802.1X authentication is enabled.
- If a range of ports or link aggregates is specified with this command, any non-UNP ports within the range are skipped.

Examples

```
-> unp port 1/1/5 802.1x-authentication max-req 10
-> unp port 1/1/10-15 802.1x-authentication max-req 5
-> no unp port 1/1/5 802.1x-authentication max-req

-> unp linkagg 10 802.1x-authentication max-req 10
-> unp linkagg 2-5 802.1x-authentication max-req 5
-> no unp linkagg 10 802.1x-authentication max-req
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp 802.1x-authentication supp-timeout	Configures the number of seconds before the switch will time out an 802.1X user that is attempting to authenticate.
unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication	Configures the 802.1X authentication status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPort8021XMaxReq
```

unp 802.1x-authentication bypass-8021x

Configures whether the 802.1X authentication process is bypassed on the specified UNP port. When enabled, the 802.1X device authentication process is skipped; only MAC authentication or rule-based classification is applied to device traffic on the UNP port.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication bypass-8021x**

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication bypass-8021x**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

By default, 801.1X authentication bypass is disabled on the UNP port; 802.1X authentication is attempted first.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- This command is only allowed on UNP-enabled ports and link aggregates.
- Enabling 802.1X authentication bypass is not allowed on UNP ports that are configured with an 802.1X authentication failure policy.

Examples

```
-> unp port 1/1/5 802.1x-authentication bypass-8021x
-> no unp port 1/1/5 802.1x-authentication bypass-8021x
-> unp port 1/1/10-15 802.1x-authentication bypass-8021x
-> no unp port 1/1/10-15 802.1x-authentication bypass-8021x

-> unp linkagg 10 802.1x-authentication bypass-8021x
-> no unp linkagg 10 802.1x-authentication bypass-8021x
-> unp linkagg 2-5 802.1x-authentication bypass-8021x
-> no unp linkagg 2-5 802.1x-authentication bypass-8021x
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication	Configures the 802.1X authentication status for the UNP port.
unp mac-authentication allow-eap	Configures whether or not subsequent 802.1X authentication is attempted based on the MAC authentication results.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPort8021XBypassStatus
```

unp 802.1x-authentication failure-policy

Configures whether the switch attempts subsequent MAC authentication for a device after the initial 802.1X authentication process fails.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication failure-policy {mac}**

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x-authentication failure-policy**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
mac	Perform MAC authentication if 802.1X authentication fails.

Defaults

By default, device classification is performed after the initial 802.1X authentication process fails.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Configuring the 802.1X authentication failure policy is not allowed on UNP ports on which 802.1X authentication bypass is enabled.
- Device classification (the default) is performed based on the classification options configured for the UNP port.

Examples

```
-> unp port 1/1/5 802.1x-authentication failure-policy mac
-> no unp port 1/1/10-15 802.1x-authentication failure-policy

-> unp linkagg 10 802.1x-authentication failure-policy mac
-> no unp linkagg 2-5 802.1x-authentication failure-policy
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication	Configures the 802.1X authentication status for the UNP port.
unp 802.1x-authentication bypass-8021x	Configures the 802.1X bypass operation status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPort8021XFailurePolicy
```

unp mac-authentication

Configures the status of MAC authentication for the specified UNP port. Enable this functionality to invoke MAC-based authentication for devices connected to the UNP port.

unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} mac-authentication**

no unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} mac-authentication**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, MAC authentication is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable MAC authentication on a UNP port or link aggregate.
- This command is only allowed on UNP-enabled ports (both bridge and access port types).
- MAC-based authentication is supported only through a RADIUS server.
- An option exists to classify a device into an alternate UNP in the event successful MAC authentication does not return a UNP name.
- If MAC authentication fails, any classification rules configured for the UNP port are applied.
- If UNP MAC authentication, 802.1X authentication, and classification (see **unp classification** and **unp 802.1x-authentication**) are disabled on the UNP port, all MAC addresses received on that port are blocked unless a default UNP is configured and/or trust VLAN tag is enabled for the port.
- Configuring an authentication server down UNP (see **unp auth-server-down)** is highly recommended when MAC or 802.1X authentication is enabled on VLAN bridge or SPB access ports or aggregates. This is because after a switch reload, traffic from devices connected to these types of ports and aggregates reaches the switch and triggers the authentication process before route convergence has completed and the server can be reached.
  - If an authentication server down UNP is configured, devices are temporarily learned in that profile and authentication is automatically attempted again after the timeout period expires. This allows time for the server to become reachable from the switch after a reload.

- If an authentication server down UNP is not configured, devices are learned as filtering and will remain in that state. There is no further attempt to authenticate these devices again.
- The authentication server down functionality is *not* supported on VXLAN access ports or aggregates.

Examples

```
-> unp port 1/1 mac-authentication
-> no unp port 1/1 mac-authentication
-> unp linkagg 2 mac-authentication
-> no unp linkagg 2 mac-authentication
```

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R02; **linkagg** parameter added.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp mac-authentication pass-alternate	Assigns the device to another VLAN-based or service-based UNP when successful MAC authentication does not return a UNP name.
unp classification	Configures the classification status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortMacAuthFlag
```

unp mac-authentication pass-alternate

Configures the name of an existing VLAN-based or service-based UNP to use as an alternate profile. A device is assigned to the alternate profile when successful MAC authentication does not return a UNP name.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} mac-authentication pass-alternate** *profile_name*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} mac-authentication pass-alternate**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
profile_name	The name of an existing VLAN, SPB, or VXLAN profile.

Defaults

By default, no alternate UNP is configured.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the alternate profile from the UNP port configuration.
- Service-based profiles classify traffic received on UNP access ports; VLAN-based profiles classify traffic received on UNP bridge ports. Make sure the specified port is of the correct type for the specified profile.
- The UNP name specified with this command must already exist in the switch configuration.

Examples

```
-> unp port 1/1 mac-authentication pass-alternate Finance
-> unp port 1/1-3 mac-authentication pass-alternate CustomerA
-> unp port 1/4-10 mac-authentication pass-alternate CustomerC
-> no unp port 1/1-3 mac-authentication pass-alternate

-> unp linkagg 5 mac-authentication pass-alternate AltUNP
-> unp linkagg 1-5 mac-authentication pass-alternate CustomerB
-> unp linkagg 10-12 mac-authentication pass-alternate CustomerD
-> no linkagg 5 mac-authentication pass-alternate
```

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R02; **linkagg** parameter added.
Release 7.3.1; **spb-profile** parameter added, **unp-name** parameter changed to **vlan-profile**.
Release 7.3.4; **vxlan-profile** parameter added.
Release 8.3.1; **vlan-profile**, **spb-profile**, and **vxlan-profile** parameters deprecated.

Related Commands

unp profile	Configures a UNP profile that is used to classify traffic received on UNP ports.
unp port-type	Configures UNP functionality on a port or link aggregate.
unp mac-authentication	Configures the MAC authentication status for the UNP port.
show unp port	Displays the UNP port parameter configuration.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortPassAltProfileName
```

unp mac-authentication allow-eap

Configures whether the switch attempts subsequent 802.1X authentication for a device connected to a UNP port on which 802.1X authentication bypass is enabled. When 802.1X bypass is enabled on the port, MAC authentication is performed first on any device connected to that port. This command specifies the conditions under which 802.1X authentication is performed or bypassed after the initial MAC authentication process.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} mac-authentication allow-eap {pass | fail | noauth}**

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} mac-authentication allow-eap**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
pass	Perform 802.1X (EAP frame) authentication if the device passes MAC authentication.
fail	Perform 802.1X (EAP frame) authentication if the device fails MAC authentication.
noauth	Perform 802.1X (EAP frame) authentication if MAC authentication is not configured on the UNP port.

Defaults

By default, the allow 802.1X authentication option is not set.

Platforms Supported

OmniSwitch 6860, 6865, 6900

Usage Guidelines

- Use the **no** form of this command to set the allow 802.1X authentication option back to the default value of none (option is not set).
- The port specified with this command must also have 802.1X bypass enabled (see the **unp 802.1x-authentication bypass-8021x** command). If bypass is not enabled, the option configured with this command does not apply.
- This command is only allowed on UNP-enabled ports and link aggregates.

Examples

```
-> unp port 1/1/5 mac-authentication allow-eap pass
-> unp port 1/1/10-15 mac-authentication allow-eap fail
-> no unp port 1/1/5 mac-authentication allow-eap
```

```
-> unp linkagg 10 mac-authentication allow-eap noauth
-> unp linkagg 2-5 mac-authentication allow-eap none
-> no unp linkagg 10 mac-authentication allow-eap
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication bypass-8021x	Configures the 802.1X bypass operation status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortMacAllowEap
```

unp classification

Configures the classification status for the specified UNP port. When classification is enabled but authentication is disabled or fails, UNP classification rules (such as MAC address, MAC address range, IP network address, or VLAN tag) are applied to the traffic received on the UNP port.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} classification**

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} classification**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (10-20).

Defaults

By default, classification is enabled on the UNP port.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the classification status for a UNP port or link aggregate.
- This command is allowed only on UNP-enabled ports (both bridge and access ports).
- UNP classification rules are applied if authentication is disabled on the port, is enabled on the port but the RADIUS server is not configured, or the authentication method fails.
- If untagged device traffic does not match any of the classification rules, the device is assigned to the default UNP configured for the port.
- If tagged device traffic does not match any of the classification rules and the trust VLAN tag option (see **unp trust-tag**) is enabled for the port, the device is classified based on the VLAN tag of the traffic if a VLAN matching the tag exists in the switch configuration.
- If all of the UNP authentication methods *and* UNP classification are disabled for the UNP port, then all MAC addresses received on that port are blocked unless a default VLAN is specified and/or trust VLAN tag is enabled for the port.

- When classification is enabled for the port, UNP classification rules are applied in the following order of precedence:
  - MAC address + VLAN tag
  - MAC address
  - MAC address range + VLAN tag
  - MAC address range
  - IP address + VLAN tag
  - IP address
  - VLAN tag

Examples

```
-> unp port 1/1 classification
-> no unp port 1/1 classification
-> unp port 1/1-4 classification
ERROR: Port 1/3 is not a unp-port
-> unp linkagg 5 classification
-> no unp linkagg 5 classification
```

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R02; **linkagg** parameter added.

Related Commands

show unp classification	Displays the UNP classification rule configuration for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortClassificationFlag
```

unp trust-tag

Configures the option of whether or not to trust the VLAN ID of a tagged packet to determine how the packet is classified.

unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} trust-tag**

no {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} trust-tag**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (10-20).

Defaults

By default, the trust VLAN tag option is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the trust tag status for a UNP port or link aggregate.
- When this option is enabled, the device is classified into a VLAN or service access point (SAP) when one of the following conditions occur:
  - MAC or 802.1X authentication passes, but the RADIUS server returns a UNP that does not exist in the switch configuration.
  - MAC or 802.1X authentication passes, but the RADIUS server does not return a UNP and the alternate UNP option is disabled for the port.
  - Device traffic does not match any of the classification rules configured for the UNP port.
  - The UNP VLAN obtained from a matching classification rule does not exist in the switch configuration.
  - Auth-Server-Down UNP option is used, but the VLAN associated with that UNP does not exist in the switch configuration.
- When the trust tag option is triggered on a UNP bridge port and a VLAN exists in the switch configuration that matches the VLAN tag, a VLAN-port-association (VPA) is created between the UNP port and the matching VLAN even if the matching VLAN is *not* associated with a UNP.
- When the trust tag option is triggered on a UNP access port, the VLAN tag information is used to create a dynamic SAP (virtual port) to which the access port is associated.
- Enabling the trust VLAN ID tag option provides an implicit method of VLAN tag classification that will accept tagged traffic matching any of the existing UNPs without the need to create specific classification rules for those profiles.

Examples

```
-> unp port 1/1 trust-tag
-> unp port 1/1-4 trust-tag
-> no unp port 1/1 trust-tag

-> unp linkagg 5 trust-tag
-> unp linkagg 6-10 trust-tag
-> no unp linkagg 5 trust-tag
```

Release History

Release 7.2.1; command was introduced.

Related Commands

show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortTrustTagStatus
```

unp default-profile

Configures the name of an existing UNP classification profile to serve as the default UNP for the specified UNP port or link aggregate.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} default-profile** *profile_name*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***} default-profile**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
*slot/port***[-***port2***]**	The slot and port number (3/1) of a UNP-enabled port. Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
profile_name	The name of an existing UNP classification profile.

Defaults

By default, there is no default profile configured for UNP ports or link aggregates.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove the default UNP from the port configuration.
- This command is allowed only on UNP-enabled ports.
- The UNP classification profile specified with this command must already exist in the switch configuration.
- The default UNP is used to classify devices on the port when one of the following conditions occur:
  - UNP authentication and classification are not enabled on the port.
  - MAC authentication fails.
  - Device traffic does not match any UNP classification rules.
  - The UNP trust VLAN tag option (see **unp trust-tag**) is enabled for the port, but the VLAN ID specified in the tag field of the device traffic does not exist in the switch configuration.
  - Untagged device traffic is not classified.

Examples

```
-> unp port 1/1 default-profile Sales
-> no unp port 1/1 default-profile
-> unp port 1/1-4 default-profile Sales
ERROR: Port 1/2 is not a unp port
ERROR: Port 1/3 is not a unp port
```

```
-> unp port 1/1 default-profile BAD-UNP
ERROR: UNP doesn't exist
-> no unp port 1/1-4 default-profile
-> unp linkagg 5 default-profile VM1-Server1
-> no unp linkagg 5 default-profile
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile	Configures a UNP profile that is used to classify traffic received on UNP ports.
unp port-type	Configures the status of UNP functionality on the port.
unp trust-tag	Configures whether or not a device is classified into an existing VLAN that matches the VLAN ID tag of the packets received from the device.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
```

unp domain

Assigns a UNP port or link aggregate to a customer domain (UNP group).

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} domain** *domain_id*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} domain** *domain_id*

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
domain_id	The numerical domain ID to which the specified port or link aggregate is assigned.

Defaults

By default, all UNP ports are assigned to customer domain zero (0).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The domain ID specified with this command must already exist in the switch configuration.
- Customer domains are used to group physical UNP ports or link aggregates into one logical domain.
- Once a port is assigned to a specific customer domain, only classification rules associated with the same customer domain ID are applied to that port.

Examples

```
-> unp port 1/1 domain 1
-> unp port 1/1-3 domain 2
-> no unp port 1/1 domain 1
-> unp linkagg 5 domain 5
-> unp linkagg 8-10 domain 6
-> no unp linkagg 5 domain 5
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp port-type	Configures the status of UNP for the specified port or link aggregate.
unp domain description	Creates a customer domain ID.
show unp domain	Displays the available customer domain IDs.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDomainId
```

unp aaa-profile

Assigns the name of an existing authentication, authorization, and accounting (AAA) profile to the specified UNP port or link aggregate. This type of profile defines AAA configuration options (such as RADIUS servers and RADIUS client attributes) that are applied to device traffic received on the UNP port to which the profile is assigned.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} aaa-profile** *profile_name*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} aaa-profile**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
profile_name	The name of an existing AAA profile.

Defaults

By default, there is no AAA profile assigned to UNP ports or link aggregates. The global AAA configuration for the switch is applied.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove the AAA profile from the port configuration.
- The AAA profile specified with this command must already exist in the switch configuration.
- AAA profiles are configured using the **aaa profile** command. See the “AAA Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide* for more information.

Examples

```
-> unp port 1/1/5 aaa-profile A1
-> no unp port 1/1/5 aaa-profile

-> unp port 1/1/1-5 aaa-profile A2
-> no unp port 1/1/1-5 aaa-profile

-> unp linkagg 10 aaa-profile A3
-> no unp linkagg 10 aaa-profile
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp port-type	Configures UNP functionality for the specified port or link aggregate.
aaa profile	Configures an AAA configuration profile.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortAaaProfile
```

unp port port-template

Assigns the name of an existing port template to the specified UNP port or link aggregate. A port template defines UNP port configuration options (such as the type of authentication, classification status, a default profile) that are applied to the UNP port to which the template is assigned.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} port-template** *template_name*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} port-template**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
template_name	The name of an existing port template.

Defaults

By default, the “bridgeDefaultPortTemplate” port template is assigned to UNP bridge ports, and the “accessDefaultPortTemplate” port template is assigned to UNP access ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove the port template from the port configuration.
- When a custom template is removed from a UNP port, the port reverts back to using the default template to define UNP port parameter options.
- The port template specified with this command must already exist in the switch configuration.
- When a port template is applied to a UNP port, the parameter values defined in the template will override any existing UNP port configuration. In addition, any attempt to explicitly configure a port that is associated with a template is not allowed.

Examples

```
-> unp port 1/1/5 port-template up1
-> unp port 1/1/1-5 port-template up2
-> no unp port 1/1/5 port-template
-> no unp port 1/1/1-5 port-template

-> unp linkagg 10 port-template up3
-> unp linkagg 10-50 port-template up4
-> no unp linkagg 10 port-template
-> no unp linkagg 10-50 port-template
```

```
-> unp port 1/10 802.1x-authentication
ERROR: Port Template already enforced on port, please remove it for manual config
on Port
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp port-type	Configures the UNP status and port type for the specified port or link aggregate.
unp port-template	Configures a port template.
show unp port config	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortPortTemplate
```

unp direction

Configures whether network access control is applied to both incoming and outgoing traffic or only applied to incoming traffic on the specified UNP bridge port or link aggregate.

unp {port *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} direction {both | in}**

no unp {port *chassis//slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} direction**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
both	Enables bidirectional network access control on the specified port or link aggregate.
in	Enables network access control for incoming traffic only on the specified port or link aggregate.

Defaults

By default, bidirectional network access control is enabled on the port.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to set the network access control direction to the default (**both**).
- When the port control direction is set to **both**, egress broadcast, unknown unicast, and multicast traffic is blocked on the UNP port.
- When the port control direction is set to **in**, egress broadcast, unknown unicast, and multicast traffic is allowed on the UNP port.
- This command applies only to ports and link aggregates configured as UNP bridge ports; this command does not apply to UNP access ports.

Examples

```
-> unp port 1/1/5 direction in
-> unp port 1/1/10-15 direction both
-> no unp port 1/1/10-15 direction

-> unp linkagg 10 direction in
-> unp linkagg 2-5 direction both
-> no unp linkagg 2-5 direction
```

Release History

Release 7.3.4; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
unp 802.1x-authentication	Configures the 802.1X authentication status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortAdminControlledDirections
```

unp admin-state

Enables or disables the UNP configuration for a port or link aggregate.

unp {port {*chassis/slot/port1***[-***port2***] | linkagg** *agg_id1***[-***agg_id2***]} admin-state {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id1***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (5-10).
enable	Activates the UNP configuration for the UNP port or link aggregate. UNP functionality is applied to traffic received on the UNP port or link aggregate.
disable	Disables the UNP configuration for the UNP port or link aggregate. UNP functionality is not applied to traffic received on the UNP port or link aggregate.

Defaults

By default, UNP is administratively enabled at the time UNP functionality is configured for the port or link aggregate.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When UNP functionality is disabled, the UNP configuration for the port or link aggregate is retained but is not applied to traffic received on the port or link aggregate.

Examples

```
-> unp port 1/1 admin-state disable
-> unp port 1/2-5 admin-state disable
-> unp port 1/1 admin-state enable
-> unp linkagg 5 admin-state disable
-> unp linkagg 8-10 admin-state disable
-> unp linkagg t admin-state enable
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp port-type	Configures UNP functionality for the specified port or link aggregate.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortAdminState
```

unp dynamic-service

Configures whether the System Default service profile dynamically creates an SPB Service Access Point (SAP) or a VXLAN SAP based on the traffic received on the UNP access port.

unp {port [*chassis_id/***]***slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} dynamic-service {spb | vxlan | none}**

Syntax Definitions

chassis_id	The chassis identifier when running in virtual chassis mode.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
spb	Dynamically creates an SPB SAP.
vxlan	Dynamically creates a VXLAN SAP (*supported only on OmniSwitch 6900-Q32, 6900-X72, 6900-V72, 6900-C32*).
none	No SPB or VXLAN SAP is dynamically created.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- This command applies only to ports and link aggregates configured as UNP access ports; this command does not apply to UNP bridge ports.
- Traffic received on UNP access ports that is not assigned to a user-defined service profile is assigned to the System Default service profile. The System Default profile attributes used to dynamically create a SAP for such traffic are derived based on the setting for this UNP port parameter.
  - If the dynamic service port parameter is set to SPB, then a calculated SPB control BVLAN, a calculated default I-SID number, and an incremental reserved service ID number are used to dynamically create a SAP for SPB service traffic received on the UNP access port.
  - If the dynamic service port parameter is set to VXLAN, then a calculated VNI number, a default multicast group IP address, and an incremental reserved service ID number are used to dynamically create a SAP for VXLAN service traffic received on the UNP access port.

Examples

```
-> unp port 1/1/5 dynamic-service vxlan
-> unp port 1/1/10-15 dynamic-service spb
-> unp port 1/1/10-15 dynamic-service none
-> unp linkagg 10 dynamic-service vxlan
-> unp linkagg 2-5 dynamic-service spb
-> unp linkagg 2-5 dynamic-service none
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortDynamicService
```

unp vlan

Configures an untagged or tagged VLAN-port association between the specified UNP bridge port and VLAN ID. This type of static VLAN assignment is particularly useful when connecting silent devices to UNP bridge ports.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} vlan** *vlan_id* **[-***vlan_id2***] [tagged]**

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} vlan** *vlan_id* **[-***vlan_id2***]**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP bridge port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
vlan_id **[-***vlan_id2***]**	The VLAN ID to assign to the UNP port. Use a hyphen to specify a range of VLAN IDs.
tagged	Configures a tagged VLAN association for the UNP bridge port.

Defaults

By default, no VLAN associations are configured for UNP bridge ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a VLAN association from the UNP port configuration. The **tagged** keyword is not required to remove a tagged VLAN association.
- This command applies only to ports and link aggregates configured as UNP bridge ports; this command does not apply to UNP access ports.
- When the **tagged** parameter option is not specified, the VLAN-port association created is untagged.
- Configuring a UNP port or link aggregate with an untagged *and* tagged VLAN-port association is allowed as long as the untagged and tagged VLANs are different (for example, **unp port 1/4/45 vlan 100** and **unp port 1/4/45 vlan 200 tagged**).
- When this command is used to assign a VLAN to a UNP bridge port, the port goes into a forwarding state for egress traffic associated with the VLANs assigned to the port. This automatically occurs even when there is no MAC address learned on the UNP port in the assigned VLANs and regardless of the direction value (in or both) set for the port.

Examples

```
-> unp port 1/1/5 vlan 500
-> unp port 1/1/5 vlan 600 tagged
-> unp port 1/1/10 vlan 100-105
-> unp port 1/1/10 vlan 200-205 tagged
```

```
-> no unp port 1/1/5 vlan 500
-> no unp port 1/1/5 vlan 600
-> no unp port 1/1/10 vlan 100-105
-> no unp port 1/1/10 vlan 200-205

-> unp linkagg 10 vlan 500
-> unp linkagg 10 vlan 600 tagged
-> unp linkagg 20 vlan 100-105
-> unp linkagg 20 vlan 200-205 tagged
-> no unp linkagg 10 vlan 500
-> no unp linkagg 10 vlan 600
-> no unp linkagg 20 vlan 100-105
-> no unp linkagg 20 vlan 200-205
```

Release History

Release 8.2.1; command was introduced.
Release 8.5R4; **tagged** parameter added.

Related Commands

unp port-type	Configures UNP functionality on a port or link aggregate.
show unp port configured-vlans	Displays the VLAN assignments configured for UNP bridge ports or link aggregates.

MIB Objects

```
alaDaUNPPortVlanTable
   alaDaUNPPortVlanVID
```

unp port profile

Configures a UNP service profile as a static profile for the specified UNP port. This type of profile assignment is particularly useful for silent devices that are connected to a UNP port; the profile SAP won't age out when the device goes idle.

unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} profile** *profile_name*

no unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} profile** *profile_name*

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
profile_name	The name of an SPB, VXLAN, or L2 GRE service profile to statically assign to the specified UNP port.

Defaults

By default, no static profile is configured for UNP ports.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a static profile association from the UNP port configuration.
- When a MAC address is learned on a UNP port and classified into a service profile, a SAP is dynamically created based on the parameter values of the service profile. Once the MAC address associated with the dynamic SAP ages out, the SAP ages out as well. To accommodate silent devices, use this command to assign a service profile to the UNP port. This will dynamically create a persistent SAP that will not age out when the device MAC address ages out; the SAP continues to receive broadcast and multicast packets for the silent device.
- Make sure the specified UNP profile name already exists in the switch configuration and is mapped to an SPB, VXLAN, L2 GRE, or static service.
  - Profiles mapped to SPB, VXLAN, or static services are configured as static profiles on UNP access ports.
  - Profiles mapped to an L2 GRE service are configured as static profiles on UNP bridge ports.
- There can be up to eight SPB or VXLAN service profiles statically assigned to one UNP access port, but mixing service types on the same port is not supported. For example, configure only eight SPB service profiles or eight VXLAN service profiles.
- There can only be one L2 GRE service profile statically assigned to a UNP bridge port.

Examples

```
-> unp port 1/1/5 profile static-spb1
-> unp port 1/1/5 profile static-spb2
-> unp port 1/1/10 profile static-vxlan1
-> unp port 1/1/10 profile static-vxlan2
-> unp port 1/1/20 profile static-l2gre1
-> no unp port 1/1/20 profile static-l2gre1

-> unp linkagg 10 profile static-spb1
-> unp linkagg 20 profile static-vxlan1
-> unp linkagg 30 profile static-l2gre1
-> no unp linkagg 30 profile static-l2gre
```

Release History

Release 8.5R4; command was introduced.

Related Commands

unp profile map service-type spb	Configures the mapping of SPB parameters to the specified UNP profile.
unp profile map service-type vxlan	Configures the mapping of VXLAN parameters to the specified UNP profile.
unp profile map service-type l2gre	Configures the mapping of an L2 GRE tunnel to the specified UNP profile.
unp profile map service-type static	Configures the mapping of an existing SPB or VXLAN service ID to the specified UNP profile.
show unp port profile	Displays the UNP service profiles that are statically assigned to UNP ports or link aggregates.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortProfile
```

unp port ap-mode

Configures the status of the Access Point (AP) mode for the specified UNP bridge port or link aggregate.

unp {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} ap-mode**

no unp {port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]} ap-mode**

Syntax Definitions

*chassis/slot/port***[**-*port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP bridge port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number for a specific UNP link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

By default, the AP mode status for the port or link aggregate is set to the global AP mode status when UNP is enabled on the port or link aggregate. For example, if the global status is disabled, the port-level status is initially disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the AP mode is enabled on the specified UNP bridge port and an AP device is detected on that port, the following actions are triggered to automatically change the operational status of the specified options (the operational status overrides the configured status):
  - The transmission of LLDP Port VLAN ID and AP Location TLVs is operationally enabled on the UNP bridge port.
  - The trust tag status for the UNP bridge port is operationally enabled.
  - The global status for dynamic VLAN configuration is operationally enabled for the switch.
- If the UNP AP mode is not enabled, the detection, learning, and management of connected OmniAccess Stellar AP devices may not occur as expected.
- AP mode functionality is not supported on UNP access ports or Learned Port Security (LPS) ports.

Examples

```
-> unp port 1/1/6 ap-mode
-> unp linkagg 10 ap-mode
-> no unp port 1/1/6 ap-mode
-> no unp linkagg 10 ap-mode
```

Release History

Release 8.6R1; command was introduced.

Related Commands

unp ap-mode	Configures the global AP mode status.
show unp port config	Displays the UNP configuration for the port.
show unp global configuration	Displays the status of UNP Layer 3 learning for the switch.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortApMode
```

unp port-template

Configures a UNP port template that is used to apply a pre-defined port configuration to a UNP port or link aggregate. Using a port template to configure UNP functionality on a port or link aggregate avoids having to configure each parameter with a separate CLI command. Applying a template configures all port-based parameters with a single CLI command.

This section describes the base command (**unp port-template**) along with optional command keywords that are used to configure port parameter values that are applied when the template is assigned to a UNP port or link aggregate. Optional keywords are listed separately but can be entered in combination on the same command line. Use the **no** form for the keywords to change a specific parameter value for the template.

There are two default port templates: "bridgeDefaultPortTemplate" (applied to UNP bridge ports) and "accessDefaultPortTemplate" (applied to UNP access ports). These templates define a default set of port parameter values that are applied at the time a port or link aggregate is configured as a UNP bridge or access port. The default templates cannot be deleted, but the template parameter values are configurable through this command.

unp port-template {*template_name* | **bridgeDefaultPortTemplate | accessDefaultPortTemplate}**
[802.1x-authentication]
[802.1x-authentication pass-alternate *profile_name***]**
[mac-authentication]
[mac-authentication pass-alternate *profile_name***]**
[classification]
[trust-tag]
[default-profile *profile_name***]**
[domain *domain_id***]**
[aaa-profile *profile_name***]**
[redirect port-bounce]
[direction {in | both}]
[802.1x-authentication tx-period *seconds***]**
[802.1x-authentication supp-timeout *seconds***]**
[802.1x-authentication max-req *max_req***]**
[802.1x-authentication bypass]
[802.1x-authentication failure-policy {mac}]
[mac-authentication allow-eap {pass | fail | noauth}]
[force-l3-learning [port-bounce]]
[admin-state {enable | disable}
[dynamic-service {spb | vxlan}
[vlan *vlan_id* **[-***vlan_id2***] [tagged]**
[l2-profile *l2profile_name***]**
[profile *profile_name***]**
[ap-mode]

no unp port-template *template_name* **[802.1x-authentication | 802.1x authentication pass-alternate | mac-authentication | mac-authentication pass-alternate | ...]**

Syntax Definitions

template_name	The name to associate with the UNP port template.
bridgeDefaultPortTemplate	The name of the default port template applied to UNP bridge ports.
accessDefaultPortTemplate	The name of the default port template applied to UNP access ports. *This parameter is currently not supported on an OmniSwitch 6465 or OmniSwitch 6560.*

Defaults

The following table contains the default values for the system-defined port templates (“accessDefaultPortTemplate” and “bridgeDefaultPortTemplate”):

parameter	system-defined port template values
802.1x-authentication	enabled
802.1x-authentication pass-alternate *profile_name*	none
mac-authentication	enabled
mac-authentication pass-alternate *profile_name*	none
classification	enabled
trust-tag	disabled
default-profile *profile_name*	none
domain *domain_id*	0
aaa-profile *profile_name*	none
redirect port-bounce	disabled
direction {in | both}	both
802.1x-authentication tx-period *seconds*	30
802.1x-authentication supp-timeout *seconds*	30
802.1x-authentication max-req *max_req*	2
802.1x-authentication bypass	disabled
802.1x-authentication failure-policy {mac}	default
mac-authentication allow-eap {pass | fail | noauth}	none
force-l3-learning [port-bounce]	disabled port bounce is enabled
admin state {enable | disable}	enabled
dynamic-service {vxlan | spb}	none for UNP bridge port template SPB for UNP access port template
vlan *vlan_id* **[-***vlan_id2***] [tagged]**	none
l2-profile *l2profile_name*	unp-def-access-profile

parameter	system-defined port template values
ap-mode	enabled
profile *profile_name*	none

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a port template from the switch configuration.
- To change the value of a specific port template parameter, specify the parameter keyword with this command. For example, **no unp port-template port1 mac-authentication**, **unp port-template port1 domain 2**, or **unp port-template port1 default-profile defprof1**. The new parameter values are applied to all UNP ports to which the template is assigned.
- The **l2-profile** port template parameter is not supported on the OmniSwitch 9900.
- If the name of the template does not exist when this command is used to modify a port parameter, the switch will automatically create a new template using the name specified. For example, the **unp port-template port1 mac-authentication** command will create the "port1" template if it does not already exist in the switch configuration.
- When a port template is applied to a UNP port, the parameter values defined in the template will override any existing UNP port configuration. In addition, any attempt to explicitly configure a port that is associated with a template is not allowed.
- For more information about specific port parameter values, refer to the following explicit UNP port configuration commands for each template parameter:

Port Template Parameter	Explicit Port Configuration Command
[802.1x-authentication]	**unp 802.1x-authentication**
[802.1x-authentication pass-alternate *profile_name***]**	**unp 802.1x-authentication pass-alternate**
[mac-authentication]	**unp mac-authentication**
[mac-authentication pass-alternate *profile_name*]	**unp mac-authentication pass-alternate**
[classification]	**unp classification**
[default-profile *profile_name***]**	**unp default-profile**
[domain *domain_id***]**	**unp domain**
[aaa-profile *profile_name***]**	**unp aaa-profile**
[redirect port-bounce]	**unp redirect port-bounce**
[direction {in | both}	**unp direction**
[802.1x-authentication tx-period *seconds***]**	**unp 802.1x-authentication tx-period**
[802.1x-authentication supp-timeout *seconds*]	**unp 802.1x-authentication supp-timeout**
[802.1x-authentication max-req *max_req***]**	**unp 802.1x-authentication max-req**
[802.1x-authentication bypass]	**unp 802.1x-authentication bypass-8021x**

Port Template Parameter	Explicit Port Configuration Command
[802.1x-authentication failure-policy {mac}	**unp 802.1x-authentication failure-policy**
[mac-authentication allow-eap {pass | fail | noauth}]	**unp mac-authentication allow-eap**
[force-l3-learning [port-bounce]	**unp force-l3-learning**
[trust-tag]	**unp trust-tag**
[admin-state {enable | disable}]	**unp admin-state**
[dynamic-service {spb | vxlan}]	**unp dynamic-service**
[vlan *vlan_id* **[-***vlan_id2***] [tagged]**	**unp vlan**
[l2-profile *l2profile_name***]**	**unp l2-profile**
[ap-mode]	**unp port ap-mode**
[profile *profile_name***]**	**unp port profile**

Examples

```
-> unp port-template port1
-> unp port-template port1 mac-authentication
-> unp port-template port1 mac-authentication pass-alternate unp1
-> unp port-template port1 classification
-> no unp port-template port1 mac-authentication
-> no unp port-template port1
-> unp port-template port2 802.1x-authentication
-> unp port-template port2 classification
-> unp port-template port2 domain 10
-> no unp port-template port2 classification
-> no unp port-template port2
```

Release History

Release 8.3.1; command was introduced.
Release 8.3.1.R02; **force-l3-learning** parameter added.
Release 8.4.1; **l2-profile** parameter added.
Release 8.5R4; **profile** parameter added, **tagged** option added to **vlan** parameter.
Release 8.6R1; **ap-mode** parameter added.

Related Commands

unp port port-template	Assigns a port configuration template to a UNP port.
show unp port config	Displays the UNP configuration for the port, including the name of the port template associated with the port, if any.
show unp port-template	Displays the port template configuration.

MIB Objects

```
alaDaUNPPortTemplateTable
  alaDaUNPPortTemplateName
  alaDaUNPPortTemplateAdminState
  alaDaUNPPortTemplateDirection
  alaDaUNPPortTemplateDomainID
  alaDaUNPPortTemplateClassification
  alaDaUNPPortTemplateTrustTag
  alaDaUNPPortTemplateDynamicService
  alaDaUNPPortTemplateDefaultProfile
  alaDaUNPPortTemplateAAAProfile
  alaDaUNPPortTemplateRedirectPortBounce
  alaDaUNPPortTemplate8021XAuth
  alaDaUNPPortTemplate8021XAuthPassAlternate
  alaDaUNPPortTemplate8021XAuthBypass
  alaDaUNPPortTemplate8021XAuthFailPolicy
  alaDaUNPPortTemplate8021XAuthTxPeriod
  alaDaUNPPortTemplate8021XAuthSuppTimeout
  alaDaUNPPortTemplate8021XAuthMaxReq
  alaDaUNPPortTemplateMACAuth
  alaDaUNPPortTemplateMACAuthPassAlternate
  alaDaUNPPortTemplateMACAuthAllowEAP
  alaDaUNPPortTemplateForceL3Learning
  alaDaUNPPortTemplateForceL3LearningPortBounce
  alaDaUNPPortTemplateL2Profile
  alaDaUNPPortTemplateApMode
alaDaUNPPortTemplateVlanTable
  alaDaUNPPortTemplateVlanVID
alaDaUNPPortTemplateProfileTable
  alaDaUNPPortTemplateProfile
```

unp network-group

Configures a network group name and its associated IPv4 addresses. The group is used to specify source or destination IP networks for UNP router domain authentication. Users attempting to access networks defined in this group are challenged for authentication.

unp network-group *net_group_name ip_address* **[mask** *net_mask***] [***ip_address2* **[mask** *net_mask2***]...]**

no unp network-group *net_group_name* **[***ip_address* **[mask** *net_mask***] [***ip_address2* **[mask** *net_mask2***]...]**

Syntax Definitions

net_group_name	The name of the network group (up to 31 alphanumeric characters).
ip_address	An IPv4 address included in the network group.
net_mask	The mask for the IPv4 address. If no mask is entered, the IPv4 address is assumed to be a host address.
ip_address2	Optional. Another IPv4 address to be included in the network group. Multiple IPv4 addresses (up to a maximum of five) may be configured for a network group. Separate each address/mask combination with a space.
net_mask2	Optional mask for the IPv4 address. If no mask is entered, the natural mask for the address will be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a network group from the configuration or to remove an IP address from a network group.
- The network group defined with this command is used to configure a router authentication condition that will trigger authentication for user traffic that matches the IPv4 networks defined in the group.
- Make sure that the IP networks/masks specified for a network group do not overlap.

Examples

```
-> unp network-group net-grp1 10.10.12.5 mask 255.255.0.0
-> unp network-group net-grp1 20.10.12.5 mask 255.255.0.0 10.50.3.1
-> unp network-group net-grp1 30.12.12.5

-> unp network-group net-grp1 10.10.12.5 mask 255.255.0.0 20.10.12.5 mask
255.255.0.0 10.50.3.1 30.12.12.5

-> no unp network-group net-grp1 10.10.12.5
```

```
-> no unp network group net-grp1
```

Release History

Release 8.5R4; command was introduced.

Related Commands

unp router-auth user-group	Configures a user group as a condition for Layer 3 authentication. A network group is specified when this type of condition is configured.
unp router-auth cp-profile	Configures a Captive Portal profile for router authentication.
unp router-auth user flush	Performs a MAC address flush of the specified router domain authentication users.
show unp network-group	Displays the UNP network group configuration.

MIB Objects

```
alaDaUNPNetworkGroupTable
   alaDaUNPNetworkGroupName
   alaDaUNPNetworkGroupIpAddrType
   alaDaUNPNetworkGroupIpAddr
   alaDaUNPNetworkGroupIpMask
```

unp router-auth user-group

Configures a user group as a condition for Layer 3 authentication. A user group specifies a destination network group and an optional source network group; traffic matching the networks in these groups is subject to router domain authentication.

unp router-auth user-group *user_group_name* **{[src-network-group** *net_group***] dst-network-group** *net_group_name***}**

no unp router-auth user-group *user_group_name*

Syntax Definitions

user_group_name	The name of the router authentication condition (up to 31 alphanumeric characters).
net_group_name	The name of an existing network group (configured through the **unp network-group** command).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove a router authentication user group from the switch configuration.
- Make sure the network group specified with this command exists in the switch configuration before attempting to configure the router authentication user group.
- To configure an optional source network group; specify the source network group name first then the destination network group name.
- When the first router authentication user group is configured, the router domain authentication feature is enabled for the switch.
- HTTP/HTTPS traffic that matches a user group condition is challenged with Captive Portal authentication; other IPv4 traffic that matches a user group condition is challenged with IP-based authentication.
- Configuring multiple router authentication user groups is allowed.
  - Any two user groups can share the same source network group as long as the destination network group for each user group is different and the IP addresses do not overlap.
  - Any two user groups can share the same destination network group as long as the source network group for each user group is different and the IP addresses do not overlap.

Examples

```
-> unp router-auth user-group ra-ugrp1 src-network-group net-grp1 dst-network-group
net-grp2
-> unp router-auth user-group ra-ugrp2 dst-network-group net-grp3

-> no unp router-auth user-group ra-ugrp1
-> no unp router-auth user-group ra-ugrp2

-> unp router-auth user-group ra-ugrp1 dst-network-group grp5
ERROR: Dst Network Group does not exist
-> unp router-auth user-group ra-ugrp2 src-network-group grp5 dst-network-group
net-grp2
ERROR: Src Network Group does not exist
```

Release History

Release 8.5R4; command was introduced.

Related Commands

unp network-group	Configures a network group name and its associated IPv4 addresses.
unp router-auth cp-profile	Configures a Captive Portal profile for router authentication.
unp router-auth user flush	Performs a MAC address flush of the specified router domain authentication users.
show unp router-auth user-group	Displays the router authentication user group configuration.

MIB Objects

```
alaDaUNPRouterAuthUserGroupTable
   alaDaUNPRouterAuthenticationName
   alaDaUNPRouterAuthenticationSrcGroup
   alaDaUNPRouterAuthenticationDestGroup
```

unp router-auth cp-profile

Specifies an existing Captive Portal (CP) profile to use for router authentication. This type of profile defines CP authentication parameter options that are applied to users that match router authentication user group conditions. If no CP profile is specified, then the global CP configuration is applied.

unp router-auth cp-profile *cp_profile_name*

no unp router-auth cp-profile *cp_profile_name*

Syntax Definitions

cp_profile_name	The name of an existing CP profile (configured through the **captive-portal-profile** command).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove the CP profile assignment.
- Make sure the CP profile name specified with this command exists in the switch configuration.
- The following global and CP profile settings are applied for CP authentication:
  - The RADIUS server to use for authentication.
  - Session timeout value (determines aging of an accept/deny entry).
  - CP maximum retry attempts (number of login attempts the user is given before access is blocked).
  - Success redirect URL (the URL to display to the client after successful CP authentication)
- The following global and CP profile settings are applied for IP-based authentication:
  - The RADIUS server to use for authentication.
  - Session timeout value (determines aging of an accept/deny entry).
- If the RADIUS server returns a session timeout value that is set to zero and the trust RADIUS option is enabled, then the session timeout for CP and IP authenticated users is set to infinity (the user session does not time out). A zero session timeout value is supported only when it is returned by the RADIUS server; setting the value to zero through the CLI is not supported.
- The router domain authentication feature is not enabled for the switch until at least one router authentication user group is configured.
- CP authentication is applied to HTTP/HTTPS traffic that matches a router authentication user group condition.

Examples

```
-> unp router-auth cp-profile cp-1
-> no unp router-auth cp-profile
```

Release History

Release 8.5R4; command was introduced.

Related Commands

unp network-group	Configures a network group name and its associated IPv4 addresses.
unp router-auth user-group	Configures a user group as a condition for Layer 3 authentication. A network group is specified when this type of condition is configured.
unp router-auth user flush	Performs a MAC address flush of the specified router domain authentication users.
show unp router-auth configuration	Displays the CP profile configuration that is used for router domain authentication.

MIB Objects

```
alaDaUNPRouterAuthenticationConfig
   alaDaUNPRouterAuthCpProfileName
```

unp router-auth user flush

Performs a MAC address flush of the specified router domain authentication users.

unp router-auth user flush {user-group *user_group_name* **| user-name** *cp_user_name* **| [ip-address** *ipv4_address* **| auth-type {cp | ip} | all}**

Syntax Definitions

user_group_name	The name of an existing router authentication user group.
cp_user_name	The Captive Portal (CP) user name.
ipv4_address	The IPv4 address associated with the router authentication user.
cp	Clears only the CP-authenticated users.
ip	Clears only the IP-authenticated users.
all	Clears all of the router authentication users.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **user-group** parameter to flush all users associated with the specified router authentication user group.
- Use the **user-name** parameter to flush the CP user name associated with the router authentication user.
- Use the **ip-address** parameter to flush the IPv4 address associated with the router authentication user.
- Use the **auth-type** parameter with the **cp** or **ip** options to flush router authentication users that were authenticated through Captive Portal or IP-based mechanisms.
- Use the **all** parameter to flush all router authentication users learned on the switch.

Examples

```
-> unp router-auth user flush all
-> unp router-auth user flush user-group ra-grp1
-> unp router-auth user flush user-name san
-> unp router-auth user flush ip-address 10.0.0.1
-> unp router-auth user flush auth-type cp
-> unp router-auth user flush auth-type ip
```

Release History

Release 8.5R4; command was introduced.

Related Commands

unp network-group	Configures a network group name and its associated IPv4 addresses.
unp router-auth user-group	Configures a user group as a condition for Layer 3 authentication. A network group is specified when this type of condition is configured.
unp router-auth cp-profile	Configures a Captive Portal profile for router authentication.
show unp router-auth users	Displays information about users authenticating through router domain authentication.

MIB Objects

```
alaDaUNPRouterAuthenticationFlushTable
   alaDaUNPRouterAuthenticationFlushIndex
   alaDaUNPRouterAuthenticationFlushComplete
   alaDaUNPRouterAuthenticationFlushUserGroupName
   alaDaUNPRouterAuthenticationFlushType
   alaDaUNPRouterAuthenticationFlushUserName
   alaDaUNPRouterAuthenticationFlushIpAddressType
   alaDaUNPRouterAuthenticationFlushIpAddress
```

show unp network-group

Displays the router authentication network group configuration.

show unp network-group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

A UNP network group is used to configure a router authentication user group condition that will trigger authentication for user traffic that matches the IPv4 networks defined in the network group.

Examples

```
-> show unp network-group
  Network Group Name      IP-Address/Mask
----------------------+-----------------------
net-grp1                10.0.0.1/255.255.0.0,
                        20.0.0.1/255.255.0.0,
                        30.0.0.1/255.0.0.0
net-grp2                40.0.0.1/255.255.0.0
net-grp3                10.0.0.1/255.255.0.0,
                        40.0.0.1/255.255.0.0

 Total Network-Group Count: 3
```

output definitions

Network Group Name	The name of the UNP network group.
IP-Address/Mask	The IPv4 network addresses that are associated with the network group name.

Release History

Release 8.5R4; command was introduced.

Related Commands

unp network-group	Configures a network group name and its associated IPv4 addresses.

MIB Objects

```
alaDaUNPNetworkGroupTable
   alaDaUNPNetworkGroupName
   alaDaUNPNetworkGroupIpAddrType
   alaDaUNPNetworkGroupIpAddr
   alaDaUNPNetworkGroupIpMask
```

show unp router-auth user-group

Displays the router authentication user group configuration.

show unp router-auth user-group [*user_group_name***]**

Syntax Definitions

user_group_name	The name of an existing router authentication user group.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

A router authentication user group specifies Layer 3 conditions for authentication; UNP network groups assigned to the router authentication user group contain IPv4 addresses. User traffic matching these networks are challenged with Captive Portal or IP-based authentication.

Examples

```
-> show unp router-auth user-group
User-Group Name                  Src-Network-Group               Dst-Network-Group
--------------------------+--------------------------+--------------------------
ra-ugrp1                    net-grp1                    net-grp2
ra-ugrp2                    net-grp3                    net-grp2
ra-ugrp3                    net-grp1                    net-grp3
ra-ugrp4                    net-grp2                    net-grp3
ra-ugrp5                                                net-grp4

-> show unp router-auth user-group UserGrp1
User-Group Name                  Src-Network-Group               Dst-Network-Group
--------------------------+--------------------------+--------------------------
ra-ugrp3                    net-grp1                    net-grp3

Rule Status = ACTIVE
```

output definitions

User-Group-Name	The name of the router authentication user group.
Src-Network-Group	The name of the UNP network group that is designated as a group of source IPv4 networks. Specifying a source network group is optional when configuring a user group condition.
Dst-Network-Group	The name of the UNP network group that is designated as a group of destination IPv4 networks.

Release History

Release 8.5R4; command was introduced.

Related Commands

unp router-auth user-group Configures a router authentication user group.

MIB Objects

```
alaDaUNPRouterAuthUserGroupTable
   alaDaUNPRouterAuthenticationName
   alaDaUNPRouterAuthenticationSrcGroup
   alaDaUNPRouterAuthenticationDestGroup
```

show unp router-auth configuration

Displays the Captive Portal (CP) profile configuration that is used for router domain authentication.

show unp router-auth configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

If no CP profile is designated for this feature, then the global CP configuration is used.

Examples

```
-> show unp router-auth configuration
       CP-Profile Name     : cp-prof1

       CP Params:
            Captive Portal AAA Profile Name        = a1
            Captive Portal Success Redirect URL    = http://server-1.com/pass.html
            Captive Portal Retry Count             = 3
```

output definitions

CP-Profile Name	The name of the Captive Portal profile to use for router authentication. Configured through the **captive-portal-profile** command.
Captive Portal AAA Profile Name	The name of the AAA profile assigned to the CP profile. The AAA profile defines the session timeout value. Configured through the **captive-portal-profile** command.
Captive Portal Success Redirect URL	The URL to which a user is redirected after successful CP authentication. Configured through the **captive-portal success-redirect-url** command.
Captive Portal Retry Count	The number of login attempts a client is allowed. Configured through the **captive-portal retry-count** command.

Release History

Release 8.5R4; command was introduced.

Related Commands

unp router-auth cp-profile	Specifies an existing CP profile to use for router authentication.

MIB Objects

```
alaDaUNPRouterAuthenticationConfig
   alaDaUNPRouterAuthCpProfileName
```

show unp router-auth users

Displays information about users authenticating through the router authentication process.

show unp router-auth users [user-name *cp_user_name***] [ip-address** *ipv4_address***] [auth-type {cp | ip}] [auth-status {pass | fail}]**

Syntax Definitions

cp_user_name	The Captive Portal (CP) user name for the router authentication user.
ipv4_address	The IPv4 address of the router authentication user.
cp	Displays only Captive Portal authenticated users.
ip	Displays only IP authenticated users.
pass	Displays only users that have successfully authenticated.
fail	Displays only users that have failed authentication.

Defaults

By default, all router authenticated users are displayed.

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the optional parameters provided with this command to filter the output display results.
- The “Username” field displays either the user name that was entered to authenticate a user device through the Captive Portal process or the IP address of the user device if IP-authentication was used to authenticate the user.

Examples

```
-> show unp router-auth users
   UserName   Destination    User-Group Intf-Name/  Auth Auth   LoginTime
              IP-Network                  Vlan      Type Status
-------------+-------------+----------+-----------+----+------+------------------
Guest-user1   70.0.0.1       DST-GRP1   L3-auth1:20  CP   Pass  06/20/2018 06:43:47
Employee-002  70.0.0.2       DST-GRP2   L3-auth2/30  CP   Fail  06/50/2018 02:00:02
40.1.1.20     70.0.0.3       DST-GRP3   L3-auth3/40  IP   Fail  07/20/2018 10:10:05
50.1.1.20     70.0.0.4       DST-GRP4   L3-auth4/50  IP   Pass  07/10/2018 05:14:10

Total users : 4

-> show unp router-auth users ip-address 40.1.1.20
   UserName   Destination    User-Group Intf-Name/  Auth Auth   LoginTime
              IP-Network                  Vlan      Type Status
-------------+-------------+----------+-----------+----+------+------------------
40.1.1.20     70.0.0.3       DST-GRP3   L3-auth3/40  IP   Fail  07/20/2018 10:10:05

Total users : 1
```

```
-> show unp router-auth users auth-type cp
   UserName   Destination    User-Group Intf-Name/  Auth Auth   LoginTime
              IP-Network                   Vlan      Type Status
-------------+-------------+----------+-----------+----+------+------------------
Guest-user1   70.0.0.1       DST-GRP1   L3-auth1:20  CP   Pass  06/20/2018 06:43:47
Employee-002  70.0.0.2       DST-GRP2   L3-auth2/30  CP   Fail  06/50/2018 02:00:02

Total users : 2

-> show unp router-auth users auth-status pass
   UserName   Destination    User-Group Intf-Name/  Auth Auth   LoginTime
              IP-Network                   Vlan      Type Status
-------------+-------------+----------+-----------+----+------+------------------
Guest-user1   70.0.0.1       DST-GRP1   L3-auth1:20  CP   Pass  06/20/2018 06:43:47
50.1.1.20     70.0.0.4       DST-GRP4   L3-auth4/50  IP   Pass  07/10/2018 05:14:10

Total users : 2
```

output definitions

UserName	Displays either the IP address or Captive Portal user name for the learned user device.
Destination IP-Network	The destination IP network address for the user device.
User-Group	The name of the router authentication user group condition that matches the user device traffic.
Intf-Name/VLAN	The name of the IP interface and VLAN associated with the user device.
Auth Type	Indicates whether the user device attempted Captive Portal or IP-based authentication.
Auth Status	Indicates whether the user device passed or failed authentication.
LoginTime	The date and time the user logged into the network.

```
-> show unp router-auth users user-name Guest-user1
User-Name                      : Guest-user1
IP-Address                     : 20.0.0.5,
Destination IP-Network         : 70.0.0.1,
Access Timestamp               : 06/20/2018 06:43:47,
Interface-Name/Vlan            : L3-auth1/20,
User-Group                     : DST-GRP1,
Authentication-Type            : CP,
Authentication-Status          : Pass,
Session-Time Remaining(sec)    : 1000 sec

-> show unp router-auth users user-name 40.1.1.20
User-Name                      : 40.1.1.20
IP-Address                     : 40.1.1.20,
   Destination IP-Network      : 70.0.0.0,
   Access Timestamp            : 07/20/2018 10:10:05,
Interface-Name/Vlan            : L3-auth3/40,
User-Group                     : DST-GRP3,
Authentication-Type            : IP,
Authentication-Status          : Fail,
Session-Time Remaining(sec)    : 200 sec
```

output definitions

UserName	Displays either the IP address or Captive Portal user name for the learned user device.
IP-Address	The IP address of the user device.
Destination IP-Network	The destination IP network address for the user device.
Access Timestamp	The date and time the user device accessed the network.
Interface-Name/VLAN	The name of the IP interface and VLAN associated with the user device.
User-Group	The name of the router authentication user group condition that matches the user device traffic.
Authentication-Type	Indicates whether the user device attempted Captive Portal or IP-based authentication.
Authentication-Status	Indicates whether the user device passed or failed authentication.
Session-Time Remaining (sec)	The amount of time remaining for the users login session.

Release History

Release 8.5R4; command was introduced.

Related Commands

unp router-auth user flush	Performs a MAC address flush of the specified router domain authentication users.

MIB Objects

N/A

unp classification port

Defines a Port classification rule for the specified UNP profile. If the UNP port or link aggregate on which the device traffic is received matches the port or link aggregate defined for the rule, the specified profile is applied to the device.

unp classification {port *chassis/slot/port1***[-***port2***] | linkagg [***agg_id***[-***agg_id2***]} [vlan-tag** *vlan_id* **|** *outer_vlan_id:inner_vlan_id***] {profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***} [profile1] [profile2] [profile3]**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
[*agg_id***[-***agg_id2***]**	The link aggregate ID for a specific UNP link aggregate. Use a hyphen to specify a range of IDs (5-10).
vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the Port rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- The Port rule configured for the specified profile is applied only to traffic learned on the specified UNP port or link aggregate.
- If a range of ports is specified with this command, any non-UNP ports within the range are skipped.
- When configuring a Port classification rule, specify and optional VLAN tag before specifying the UNP for which the rule will classify traffic.

- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).
- If a VLAN ID tag is specified with this command, the UNP is applied only to tagged packets that are received on the specified UNP port *and* that contain the VLAN ID tag.
- Untagged packets are only classified using the specified UNP port; the VLAN ID tag is ignored if it is specified with this rule.
- A Port classification rule can be combined with a MAC address rule and IP address rule to configure a port-based binding rule.

Examples

```
-> unp classification port 1/1/5 vlan-tag 100 profile1 unp1-vxlan profile2 unp2-spb
-> unp classification port 1/1/10-15 profile1 unp1-vlan profile2 unp2-spb
-> no unp classification port 1/1/5 profile2
-> no unp classification port 1/1/5

-> unp classification linkagg 5 profile1 unp1-vlan profile2 unp2-vxlan profile3
unp3-spb
-> unp classification linkagg 6-10 vlan-tag 10:20 profile1 unp1-vlan
-> no unp classification linkagg 5 profile3
-> no unp classification linkagg 5
```

Port + MAC address + IP address binding rule example:

```
-> unp classification mac-address 00:11:22:33:44:55 ip-address 10.0.0.20 mask
255.255.0.0 port 1/1/15 profile1 Pr3
-> no unp classification mac-address 00:11:22:33:44:55 ip-address 10.0.0.20 mask
255.255.0.0 port 1/1/15
```

Port + MAC address binding rule example:

```
-> unp classification mac-address 00:11:22:33:44:55 port 1/1/5 profile1 Pr1
-> no unp classification mac-address 00:11:22:33:44:55 port 1/1/5
```

Port + IP address binding rule example:

```
-> unp classification ip-address 10.0.0.20 mask 255.255.0.0 port 1/1/10 profile1
Pr2
-> no unp classification ip-address 10.0.0.20 mask 255.255.0.0 port 1/1/10
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPPortRuleTable
  alaDaUNPPortRuleNum
  alaDaUNPPortRuleVlanTag
  alaDaUNPPortRuleProfile1
  alaDaUNPPortRuleProfile2
  alaDaUNPPortRuleProfile3
```

unp classification domain

Defines a Domain ID classification rule for the specified UNP profile. If the port or link aggregate on which the device traffic is received belongs to a Domain ID that matches the Domain ID defined for the rule, the specified profile is applied to the device.

unp classification domain *domain_id* **[vlan-tag** *vlan_id* | *outer_vlan_id:inner_vlan_id***] {profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification domain *domain_id* **[profile1] [profile2] [profile3]**

Syntax Definitions

domain_id	A domain ID number.
vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the domain ID rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- When configuring a Port classification rule, specify and optional VLAN tag before specifying the UNP for which the rule will classify traffic.
- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets received on a UNP port associated with the Domain ID *and* tagged with the specified VLAN ID.
- Untagged packets are only classified using the specified domain ID; the VLAN ID tag is ignored if it is specified with this rule.
- A domain ID classification rule can be combined with a MAC address rule and an IP address rule to configure a domain-based binding rule.

Examples

```
-> unp classification domain 10 profile1 unp1-vlan
-> unp classification domain 20 vlan-tag 100 profile1 unp1-vxlan profile2 unp2-spb
profile3 unp3-vlan
-> no unp classification domain 20 profile3
-> no unp classification domain 20
```

Domain ID + MAC address + IP address binding rule example:

```
-> unp classification mac-address 00:11:22:33:44:55 ip-address 10.0.0.20 mask
255.255.0.0 domain 10 profile1 Pr3
-> no unp classification mac-address 00:11:22:33:44:55 ip-address 10.0.0.20 mask
255.255.0.0 domain 10
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainRuleTable
  alaDaUNPCustDomainRuleId
  alaDaUNPCustDomainRuleVlanTag
  alaDaUNPCustDomainRuleProfile1
  alaDaUNPCustDomainRuleProfile2
  alaDaUNPCustDomainRuleProfile3
```

unp classification mac-address

Defines a MAC address classification rule for the specified UNP. If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

unp classification mac-address *mac_address* **[domain** *domain_id***] [vlan-tag** *vlan_id* **|** *outer_vlan_id:inner_vlan_id***] {profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification mac-address *mac_address* **[profile1] [profile2] [profile3]**

Syntax Definitions

mac_address	MAC address (e.g., 00:00:39:59:f1:0c).
domain_id	An existing customer domain ID to which this rule will apply.
vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP.

parameter	default
vlan_id	none
domain_id	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the MAC address rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- When configuring a MAC address classification rule, specify and optional VLAN tag and/or an optional customer domain ID before specifying the UNP for which the rule will classify traffic.
- When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.

- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source MAC address *and* the VLAN ID tag.
- Untagged packets are only classified using the specified MAC address; the VLAN ID tag is ignored if it is configured for this rule.

Examples

```
-> unp classification mac-address 00:11:22:33:44:55 profile1 CustA
-> unp classification mac-address 00:2a:95:00:00:01 vlan-tag 200 profile1 VNP1
profile2 vxlp-1
-> unp classification mac-address 00:2b:96:11:22:03 profile1 CustA profile2 VNP1
profile3 vxlp-1
-> unp classification mac-address 00:11:22:33:44:56 domain 2 vlan-tag 100:200
profile1 CustB
-> unp classification mac-address 00:2a:95:00:00:02 domain 1 profile1 unp1-vlan
profile2 unp2-spb
-> no unp classification mac-address 00:2b:96:11:22:03 profile3
-> no unp classification mac-address 00:2a:95:00:00:02
```

Release History

Release 8.3.1; command introduced.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp domain	Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainMacRuleTable
   alaDaUNPCustDomainMacRuleDomainId
   alaDaUNPCustDomainMacRuleAddr
   alaDaUNPCustDomainMacRuleVlanTag
   alaDaUNPCustDomainMacRuleProfile1
   alaDaUNPCustDomainMacRuleProfile2
   alaDaUNPCustDomainMacRuleProfile3
```

unp classification mac-oui

Defines a MAC address Organizationally Unique Identifier (OUI) classification rule for the specified UNP profile. If the OUI of the source MAC address of the device traffic matches the OUI defined for the rule, the specified profile is applied to the device.

unp classification mac-oui *mac_oui* **[vlan-tag** *vlan_id* | *outer_vlan_id:inner_vlan_id***] {profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification mac-oui *mac_oui* **[profile1] [profile2] [profile3]**

Syntax Definitions

mac_oui	The first three octets of the MAC address (for example, e8:39:35 is the OUI of MAC address e8:39:35:10:fe:11).
vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP.

parameter	default
vlan_id	none

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the MAC OUI rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- When configuring a MAC address OUI classification rule, specify and optional VLAN tag before specifying the UNP for which the rule will classify traffic.

- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source MAC address OUI *and* the VLAN ID tag.
- Untagged packets are only classified using the specified MAC address OUI; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification mac-oui 00:11:22 profile1 unp1-vlan
-> unp classification mac-oui 00:11:33 vlan-tag 10 profile1 unp1-vlan profile2
unp2-spb profile3 unp3-vxlan
-> no classification mac-oui 00:11:33 profile3
-> no unp classification mac-oui 00:11:22
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPMacOuiRuleTable
  alaDaUNPMacOuiRuleAddr
  alaDaUNPMacOuiRuleVlanTag
  alaDaUNPMacOuiRuleProfile1
  alaDaUNPMacOuiRuleProfile2
  alaDaUNPMacOuiRuleProfile3
```

unp classification mac-range

Defines a MAC address range classification rule for the specified UNP. If the source MAC address of the device traffic matches any address within the range of MAC addresses, the specified UNP is applied to the device. An optional VLAN ID tag parameter is also available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

unp classification mac-range *low_mac_address high_mac_address* **[domain** *domain_id***] [vlan-tag** *vlan_id | outer_vlan_id:inner_vlan_id***] {profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification mac-range *low_mac_address high_mac_address* **[profile1] [profile2] [profile3]**

Syntax Definitions

low_mac_address	MAC address that defines the low end of the range (e.g., 00:00:39:59:f1:00).
high_mac_address	MAC address that defines the high end of the range (e.g., 00:00:39:59:f1:90).
domain_id	An existing customer domain ID to which this rule will apply.
vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP.

parameter	default
vlan_id	none
domain_id	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the MAC address range rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- When configuring a MAC address range classification rule, specify and optional VLAN tag and/or an optional domain ID before specifying the UNP for which the rule will classify traffic.

- When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing a source MAC address within the specified range *and* the VLAN ID tag.
- Untagged packets are only classified using the specified MAC address range; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification mac-range 00:11:22:33:44:66 00:11:22:33:44:77 profile1 CustA
-> unp classification mac-range 00:11:22:33:44:88 00:11:22:33:44:99 profile1 vNP1
profile2 vNP2 profile3 vNP3
-> unp classification mac-range 00:11:22:33:44:99 00:11:22:33:45:01 vlan-tag 20
profile1 vNP1
-> unp classification mac-range 00:11:22:33:44:01 00:11:22:33:44:20 domain 2
profile1 CustB
-> unp classification mac-range 00:11:22:33:44:01 00:11:22:33:44:20 domain 3 vlan-
tag 200 profile1 unp1-vlan profile2 unp2-spb profile3 unp3-vxlan
-> no unp classification mac-range 00:11:22:33:44:88 00:11:22:33:44:99 profile3
-> no unp classification mac-range 00:11:22:33:44:66 00:11:22:33:44:77
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp domain	Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainMacRangeRuleTable
   alaDaUNPCustDomainMacRangeRuleLoAddr
   alaDaUNPCustDomainMacRangeRuleHiAddr
   alaDaUNPCustDomainMacRangeRuleVlanTag
   alaDaUNPCustDomainMacRangeRuleDomainId
   alaDaUNPCustDomainMacRangeRuleProfile1
   alaDaUNPCustDomainMacRangeRuleProfile2
   alaDaUNPCustDomainMacRangeRuleProfile3
```

unp classification ip-address

Defines an IP network address classification rule for the specified UNP. If the source IP address of the device traffic matches the IP address defined for the rule, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source IP address.

unp classification ip-address *ip_address* **mask** *subnet_mask* **[domain** *domain_id***] [vlan-tag** *vlan_id* **|** *outer_vlan_id:inner_vlan_id***] {profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification ip-address *ip_address* **mask** *subnet_mask* **[profile1] [profile2] [profile3]**

Syntax Definitions

ip_address	IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).
subnet_mask	An IP address mask to identify the IP subnet for the interface (supports class-less masking).
domain_id	An existing customer domain ID to which this rule will apply.
vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP.

parameter	default
vlan_id	none
domain_id	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove an IP network address rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- When configuring an IP network address classification rule, specify and optional VLAN tag and/or an optional customer domain ID before specifying the UNP for which the rule will classify traffic.

- When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.
- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source IP address *and* the VLAN ID tag.
- Untagged packets are only classified using the specified IP address; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification ip-address 10.1.1.1 mask 255.255.255.0 profile1 CustA
-> unp classification ip-address 20.1.1.1 mask 255.255.0.0 profile1 vNP1 profile2
vNP2
-> unp classification ip-address 50.1.1.1 mask 255.255.255.0 vlan-tag 300 profile1
CustB
-> unp classification ip-address 60.1.1.1 mask 255.255.0.0 domain 2 profile1 unp2
profile2 unp3-spb
-> unp classification ip-address 70.1.1.1 mask 255.255.0.0 domain 1 vlan-tag 20:30
profile1 vNP3
-> no unp classification ip-address 20.1.1.1 mask 255.255.0.0 profile2
-> no unp classification ip-address 10.1.1.1 mask 255.255.255.0
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp domain	Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainIpNetRuleTable
   alaDaUNPCustDomainIpNetRuleDomainId
   alaDaUNPCustDomainIpNetRuleAddr
   alaDaUNPCustDomainIpNetRuleMask
   alaDaUNPCustDomainIpNetRuleVlanTag
   alaDaUNPCustDomainIpNetRuleProfile1
   alaDaUNPCustDomainIpNetRuleProfile2
   alaDaUNPCustDomainIpNetRuleProfile3
```

unp classification vlan-tag

Defines a VLAN tag classification rule for the specified UNP. If the VLAN ID tag of the device traffic matches the VLAN ID defined for the rule, the specified UNP is applied to the device.

unp classification vlan-tag {*vlan_id* | *outer_vlan_id***:***inner_vlan_id***]} [domain** *domain_id***] {profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification vlan-tag *vlan_id* **[profile1] [profile2] [profile3]**

Syntax Definitions

vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
domain_id	An existing customer domain ID to which this rule will apply.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP.

parameter	default
domain_id	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a VLAN tag rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- When configuring a VLAN tag classification rule, specify an optional customer domain ID before specifying the name of the UNP for which the rule will classify traffic.
- When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.

- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).
- Untagged packets are not classified with this rule.

Examples

```
-> unp classification vlan-tag 400 profile1 CustA
-> unp classification vlan-tag 10:20 domain 3 profile1 unp1 profile2 spb1
-> no unp classification vlan-tag 10:20 profile1
-> no unp classification vlan-tag 400
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp domain	Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainVlanTagRuleTable
   alaDaUNPCustDomainVlanTagRuleDomainId
   alaDaUNPCustDomainVlanTagRuleVlan
   alaDaUNPCustDomainVlanTagRuleProfile1
   alaDaUNPCustDomainVlanTagRuleProfile2
   alaDaUNPCustDomainVlanTagRuleProfile3
```

unp classification lldp med-endpoint

Defines a Link Layer Discovery Protocol (LLDP) classification rule for the specified UNP profile. This rule is used specifically for IP phones and OmniAccess Stellar Access Point (AP) devices.

unp classification lldp med-endpoint {ip-phone | access-point} {profile1 *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification lldp med-endpoint {ip-phone | access-point} [profile1] [profile2] [profile3]

Syntax Definitions

ip-phone	When LLDP TLVs from an IP phone are detected, apply the specified profile to the IP phone.
access-point	When LLDP TLVs from an OmniAccess Stellar AP are detected, apply the specified profile to the AP device.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP profile.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- There is a built-in LLDP classification rule for access points that is assigned to a built-in profile named “defaultWLANProfile”. This rule facilitates the automatic detection and classification of OmniAccess Stellar APs that are connected to UNP bridge ports. Consider the following regarding the built-in LLDP access point rule:
  - The rule cannot be removed from the switch configuration. However, the profile designation for the rule can be changed.
  - The rule does not appear in the configuration snapshot for the switch unless the profile assignment for the rule was changed.
  - When Stellar APs are detected, they are classified and assigned to the VLAN that is mapped to the built-in “defaultWLANProfile”. This VLAN serves as the management VLAN for untagged AP traffic.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.

- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

Examples

```
-> unp classification lldp med-endpoint ip-phone profile1 unp1-vlan profile2 unp2-
vlan
-> no unp classification lldp med-endpoint ip-phone profile2
-> no unp classification lldp med-endpoint ip-phone

-> unp classification lldp med-endpoint access-point profile1 defaultWLANProfile
-> no unp classification lldp med-endpoint access-point
ERROR: BUILT-IN Access-Point LLDP Rule cannot be deleted
```

Release History

Release 8.3.1; command was introduced.
Release 8.4.1.R02; **access-point** parameter added.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPEndPoinRuleTable
  alaDaUNPEndPoinRuleId
  alaDaUNPEndPoinProfile1
  alaDaUNPEndPoinProfile2
  alaDaUNPEndPoinProfile3
```

unp classification authentication-type

Defines an Authentication Type classification rule for the specified UNP profile. If the type of authentication applied to the device traffic matches the authentication type defined for the rule, the specified profile is applied to the device.

unp classification authentication-type {none | mac [fail] | 802.1x [fail]} [vlan-tag *vlan_id* **|** *outer_vlan_id:inner_vlan_id***] {profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp classification authentication-type {none | mac [fail] | 802.1x [fail]} [profile1] [profile2] [profile3]

Syntax Definitions

none	No authentication was applied to the device.
mac	The device was successfully authenticated through MAC authentication.
802.1x	The device was successfully authenticated through 802.1X authentication.
fail	Optional parameter to specify failed MAC or 802.1X authentication.
vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
profile_name	The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP profile.

parameter	default
vlan_id	none

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- The optional **fail** parameter is used only in combination with the **mac** or **802.1x** parameter. When configured, the device is checked for a failed MAC or 802.1X authentication condition to determine whether or not the profile is applied.
- When the **fail** parameter is not specified (the default), the device is checked for a successful MAC or 802.1X authentication condition to determine whether or not the profile is applied.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.

- When configuring this type of classification rule, specify an optional VLAN tag before specifying the UNP profile name for which the rule will classify traffic.
- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.
- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified authentication type *and* the VLAN ID tag.
- Untagged packets are only classified using the specified authentication type; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification authentication-type 802.1X profile1 unp1-vlan profile2 unp2-
vlan profile3 unp3-vlan
-> no unp classification authentication-type 802.1X profile2
-> no unp classification authentication-type 802.1X

-> unp classification authentication-type 802.1X fail profile1 unp1-vlan profile2
unp2-vlan profile3 unp3-vlan
-> no unp classification authentication-type 802.1X fail profile3
-> no unp classification authentication-type 802.1X fail

-> unp classification authentication-type MAC profile1 unp1-vlan profile2 unp2-vlan
profile3 unp3-vlan
-> no unp classification authentication-type MAC profile2
-> no unp classification authentication-type MAC

-> unp classification authentication-type MAC fail profile1 unp1-vlan profile2
unp2-vlan profile3 unp3-vlan
-> no unp classification authentication-type MAC fail profile3
-> no unp classification authentication-type MAC fail

-> unp classification authentication-type MAC vlan-tag 10 profile1 unp1-vlan
profile2 unp2-vlan profile3 unp3-vlan
-> no unp classification authentication-type MAC profile2
-> no unp classification authentication-type MAC
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp profile	Configures a UNP profile.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPAuthRuleTable
  alaDaUNPAuthRuleType
  alaDaUNPAuthRuleVlanTag
  alaDaUNPAuthRuleProfile1
  alaDaUNPAuthRuleProfile2
  alaDaUNPAuthRuleProfile3
```

unp classification-rule

Configures an extended classification rule name and assigns a precedence value to the specified name. This type of rule defines a list of rule conditions, all of which a device must match to be classified into the UNP profile associated with the extended rule name.

unp classification-rule *rule_name* **[precedence** *precedence_value***] [profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]]**

no unp classification-rule *rule_name* **[profile1] [profile2] [profile3]**

Syntax Definitions

rule_name	The name to associate with the extended classification rule.
precedence_value	The precedence level to assign to the extended rule. The valid range is 1–255 (1 = lowest, 255 = highest). Precedence value 255 is reserved for Device Profiling classification rules.
profile_name	The name of an existing UNP profile to assign to the extended rule.

Defaults

parameter	default
precedence_value	1
profile_name	none

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the extended rule from the switch configuration or to remove a UNP profile name assigned to the rule.
- The precedence value specified with this command is used to determine precedence among extended classification rules.
- Extended rules take precedence over all other UNP classification rules (individual rules and binding rule combinations).
- Although some individual classification rules can be combined to form a binding rule, a binding rule is not assigned a rule name and does not have a configurable precedence value. In addition, extended classification rules offer more rule combinations than binding rules.

- The following extended classification rules are automatically defined when Device Profiling is enabled for the switch (these rules cannot be removed):
  - devProfPrinter
  - devProfWindows
  - devProfIP-Phone
  - devProfWireless-Router
  - devProfSmartPhone/PDA/Tablets

Examples

```
-> unp classification-rule ext-r1
-> unp classification-rule ext-r1 profile1 UNP1 profile2 UNP2
-> unp classification-rule ext-r1 precedence 250

-> unp classification-rule ext-r2
-> unp classification-rule ext-r2 precedence 255
ERROR: Precedence 255 is reserved for Device Profiling
-> unp classification-rule ext-r2 precedence 254
-> unp classification-rule ext-r2 profile1 UNP3 profile2 UNP4 profile3 UNP5

-> no unp classification-rule ext-r1 profile1 UNP1
-> no unp classification-rule ext-r1

-> no unp classification-rule ext-r2 profile1 UNP4
-> no unp classification-rule ext-r2

-> no unp classification-rule devProfPrinter
ERROR: Device Profiling Rule cannot be modified
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; **edge-profile** parameter deprecated; **profile1**, **profile2**, and **profile3** parameters added.
Release 8.5R2; precedence value 255 reserved for Device Profiling extended classification rules.

Related Commands

unp classification-rule port	Defines a Port rule condition for an extended classification rule.
unp classification-rule domain	Defines a Group ID rule condition for an extended classification rule.
unp classification-rule mac-address	Defines a MAC address rule condition for an extended classification rule.
unp classification-rule mac-oui	Defines a MAC OUI rule condition for an extended classification rule.
unp classification-rule mac-range	Defines a MAC address range rule condition for an extended classification rule.
unp classification-rule ip-address	Defines an IP address rule condition for an extended classification rule.
unp classification-rule vlan-tag	Defines a VLAN tag rule condition for an extended classification rule.
unp classification-rule lldp med-endpoint	Defines an LLDP endpoint rule condition for an extended classification rule.
unp classification-rule authentication-type	Defines an authentication type rule condition for an extended classification rule.
unp classification-rule device-type	Defines a Device Profiling rule condition for an extended classification rule.
unp profile	Configures a UNP profile.
unp classification	Configures the classification status for the UNP port. Rules are not applied when the port classification status is disabled.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRulePrecedenceNum
  alaDaUNPClassifRuleProfile1
  alaDaUNPClassifRuleProfile2
  alaDaUNPClassifRuleProfile3
```

unp classification-rule port

Defines a Port rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **{port** *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***}**

no unp classification-rule *rule_name* **{port | linkagg}**

Syntax Definitions

rule_name	The name of an extended classification rule to which the rule condition is assigned.
*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
agg_id	Link aggregate ID.

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the Port rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

Examples

```
-> unp classification-rule ext-r1 port 1/1/10
-> no unp classification-rule ext-r1 port

-> unp classification-rule ext-r2 port 1/1/1-5
-> no unp classification-rule ext-r2 port

-> unp classification-rule ext-r3 linkagg 10
-> unp classification-rule ext-r3 linkagg
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRulePort
```

unp classification-rule domain

Defines a domain ID rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **domain** *domain_id*

no unp classification-rule *rule_name* **domain**

Syntax Definitions

rule_name	The name of an extended classification rule to which the rule condition is assigned.
domain_id	Domain ID number.

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the Domain ID rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

Examples

```
-> unp classification-rule ext-r1 domain-id GRP1
-> no unp classification-rule ext-r1 domain-id
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; **group-id** parameter changed to **domain**.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRuleCustomerDomain
```

unp classification-rule mac-address

Defines a MAC address, rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **mac-address** *mac_address*

no unp classification-rule *rule_name* **mac-address**

Syntax Definitions

rule_name	The name of an extended classification rule to which the rule condition is assigned.
mac_address	MAC address (e.g., 00:00:39:59:f1:0c).

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- Configuring all three types of MAC rules (MAC address, MAC OUI, and MAC address range) for the same extended classification rule is not allowed. Only one type of MAC rule is configurable for a given extended classification rule.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

Examples

```
-> unp classification-rule ext-r1 mac-address 00:11:22:33:44:55
-> no unp classification-rule ext-r1 mac-address
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated UNP profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRuleMacAddr
```

unp classification-rule mac-oui

Defines a MAC OUI rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **mac-oui** *mac_oui*

no unp classification-rule *rule_name* **mac-oui**

Syntax Definitions

rule_name	The name of an extended classification rule to which the rule condition is assigned.
mac_address	MAC address (e.g., 00:00:39:59:f1:0c).
mac_oui	The Organizationally Unique Identifier (OUI) of the MAC address. The OUI is the first three octets of the MAC address (for example, e8:39:35 is the OUI of MAC address e8:39:35:10:fe:11).

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- Configuring all three types of MAC rules (MAC address, MAC OUI, and MAC address range) for the same extended classification rule is not allowed. Only one type of MAC rule is configurable for a given extended classification rule.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

Examples

```
-> unp classification-rule ext-r1 mac-oui 00:11:22
-> no unp classification-rule ext-r1 mac-oui
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRuleMacOuiAddr
```

unp classification-rule mac-range

Defines a MAC address range rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **mac-range** *low_mac_address high_mac_address*

no unp classification-rule *rule_name* **mac-range**

Syntax Definitions

rule_name	The name of an extended classification rule to which the rule condition is assigned.
low_mac_address	MAC address that defines the low end of the range (for example, 00:00:39:59:f1:00).
high_mac_address	MAC address that defines the high end of the range (for example, 00:00:39:59:f1:90).

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- Configuring all three types of MAC rules (MAC address, MAC OUI, and MAC address range) for the same extended classification rule is not allowed. Only one type of MAC rule is configurable for a given extended classification rule.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

Examples

```
-> unp classification-rule ext-r1 mac-range 00:11:22:33:44:55 00:11:22:33:44:66
-> no unp classification-rule ext-r1 mac-range
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRuleMacRngLoaddr
  alaDaUNPClassifRuleMacRngHiaddr
```

unp classification-rule ip-address

Defines an IP network address rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **ip-address** *ip_address* **mask** *subnet_mask*

no unp classification-rule *rule_name* **ip-address**

Syntax Definitions

rule_name	The name of an extended classification rule to which the rule condition is assigned.
ip_address	IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).
subnet_mask	An IP address mask to identify the IP subnet for the interface (supports class-less masking).

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

Examples

```
-> unp classification-rule ext-r1 ip-address 10.0.0.20 mask 255.0.0.0
-> no unp classification-rule ext-r1 ip-address
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRuleIpAddressType
  alaDaUNPClassifRuleIpAddress
  alaDaUNPClassifRuleIpMaskType
  alaDaUNPClassifRuleIpMask
```

unp classification-rule vlan-tag

Defines a VLAN tag rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **vlan-tag [***vlan_id* | *outer_vlan_id:inner_vlan_id***]**

no unp classification-rule vlan-tag

Syntax Definitions

rule_name	The name of an extended classification rule to which the rule condition is assigned.
vlan_id	A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets. Specify a value of zero to classify untagged traffic.
outer_vlan_id:inner_vlan_id	An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

Examples

```
-> unp classification-rule ext-r1 vlan-tag 200
-> unp classification-rule ext-r2 vlan-tag 10:20
-> unp classification-rule ext-r3 vlan-tag 0
-> no unp classification-rule ext-r1 vlan-tag
```

Release History

Release 8.2.1; command was introduced.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
   alaDaUNPClassifRuleName
   alaDaUNPClassifRuleVlanTag
```

unp classification-rule lldp med-endpoint

Defines an LLDP rule condition for the specified extended classification rule name. This rule condition is specifically to detect IP phone TLVs or OmniAccess Stellar Access Point (AP) TLVs.

unp classification-rule *rule_name* **lldp med-endpoint {ip-phone | access-point}**

no unp classification-rule *rule_name* **lldp med-endpoint ip-phone**

Syntax Definitions

rule_name	The name of an extended classification rule to which the port condition is assigned.
ip-phone	When LLDP TLVs from an IP phone are detected, apply the specified profile to the IP phone.
access-point	When LLDP TLVs from an OmniAccess Stellar AP are detected, apply the specified profile to the AP device.

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.
- When using the **access-point** option to define this rule condition, make sure “defaultWLANProfile” is assigned as the profile for the specified extended classification rule name.

Examples

```
-> unp classification-rule ext-r1 lldp med-endpoint ip-phone
-> no unp classification-rule ext-r1 lldp med-endpoint ip-phone

-> unp classification-rule AP profile1 defaultWLANProfile
-> unp classification-rule AP lldp med-endpoint access-point
-> no unp classification-rule AP lldp med-endpoint access-point
```

Release History

Release 8.1.1; command was introduced.
Release 8.4.1.R02; **access-point** parameter added.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRuleEndPoin
```

unp classification-rule authentication-type

Defines an authentication type rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **authentication-type {none | mac [fail] | 802.1x [fail]}**

no unp classification-rule *rule_name* **authentication-type**

Syntax Definitions

rule_name	The name of an extended classification rule to which the port condition is assigned.
none	No authentication was applied to the device.
mac	The device was successfully authenticated through MAC authentication.
802.1x	The device was successfully authenticated through 802.1X authentication.
fail	Optional parameter to specify failed MAC or 802.1X authentication.

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.
- The optional **fail** parameter is used only in combination with the **mac** or **802.1x** parameter. When configured, the device is checked for a failed MAC or 802.1X authentication condition to determine whether or not the profile is applied.
- When the **fail** parameter is not specified (the default), the device is checked for a successful MAC or 802.1X authentication condition to determine whether or not the profile is applied.

Examples

```
-> unp classification-rule ext-r1 authentication-type 8021x
-> unp classification-rule ext-r1 authentication-type 8021X fail
-> unp classification-rule ext-r1 authentication-type mac
-> unp classification-rule ext-r1 authentication-type mac fail
-> no unp classification-rule ext-r1 authentication-type
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRuleAuthType
```

unp classification-rule device-type

Defines a Device Profiling rule condition for the specified extended classification rule name.

unp classification-rule *rule_name* **device-type** *device_name*

no unp classification-rule *rule_name* **device-type**

Syntax Definitions

rule_name	The name of an extended classification rule to which the rule condition is assigned.
device_name	The name of a device type to which the condition is assigned.

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.
- The following extended classification rules are automatically defined when Device Profiling is enabled for the switch (the device type for these rules cannot be removed):
  - devProfPrinter
  - devProfWindows
  - devProfIP-Phone
  - devProfWireless-Router
  - devProfSmartPhone/PDA/Tablets

Examples

```
-> unp classification-rule ext-r1 device-type Printer

-> no unp classification-rule ext-r1 device-type

-> no unp classification-rule devProfPrinter device-type
ERROR: Device-type cannot be modified on built-in rules
```

Release History

Release 8.5R2; command was introduced.

Related Commands

unp classification-rule	Configures an extended classification rule name and associated profile.
show unp classification-rule	Displays the UNP extended classification rule configuration.

MIB Objects

```
alaDaUNPClassifRuleTable
  alaDaUNPClassifRuleName
  alaDaUNPClassifRuleDeviceType
```

unp user-role

Configures a user-defined role name and assigns a precedence value to the specified name. This type of role is used to define a list of conditions and a QoS policy list name. If the current context of a device matches all of the role conditions, then the policy list is applied to that device.

unp user-role *role_name* **[precedence** *precedence_value***]**

no unp user-role *role_name*

Syntax Definitions

role_name	The name to associate with the user-defined role.
precedence_value	The precedence level to assign to the user-defined role. The valid range is 1–255 (1 = lowest, 255 = highest).

Defaults

parameter	default
precedence_value	**1**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the user-defined role from the switch configuration.
- The precedence value specified with this command is used to determine precedence among other user-defined roles.
- Every time the user context changes for a device, all the user-defined roles are checked to see if there is a role that matches the current user context.
- Only one user-defined role per user is allowed because only one QoS policy list per user is allowed.

Examples

```
-> unp user-role role1
-> unp user-role role2 precedence 255
-> no unp user-role role2
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp user-role policy-list	Assigns a QoS policy list to a user-defined role.
unp user-role profile	Configures a UNP profile condition for a user-defined role name.
unp user-role authentication-type	Defines an authentication type condition for a user-defined role name.
unp user-role cp-status-post-login	Configures the Captive Portal post login status as a condition for a user-defined role.
show unp user-role	Displays the user-defined role configuration for the switch.

MIB Objects

```
alaDaUNPUserRoleTable
  alaDaUNPUserRoleName
  alaDaUNPUserRolePrecedenceNum
```

unp user-role policy-list

Assigns a QoS policy list to the specified user-defined role name. When the context of a user device matches all the user-defined role conditions, the policy list associated with the role is applied to the device.

unp user-role *role_name* **policy-list** *list_name*

no unp user-role *role_name* **policy-list**

Syntax Definitions

role_name	The name of a user-defined role to which the QoS policy list is assigned.
list_name	The name of an existing QoS policy list.

Defaults

By default, no QoS policy list is assigned to a user-defined role.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a QoS policy list from the specified user-defined role.
- If the user-defined role name specified with this command does not exist, the switch will automatically create the role name and associate the QoS policy list with that name.
- The QoS policy list name specified with this command must already exist in the switch configuration.

Examples

```
-> unp user-role role1 policy-list role1-list
-> unp user-role role2 policy-list role2-list
-> no unp user-role role2 policy-list
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp user-role	Configures the name and precedence for a user-defined role.
policy list	Configures a QoS policy list.
show unp user-role	Displays the user-defined role configuration for the switch.

MIB Objects

```
alaDaUNPUserRoleTable
  alaDaUNPUserRoleName
  alaDaUNPUserRolePolicyList
```

unp user-role profile

Defines a UNP profile condition for the specified user-defined role name.

unp user-role *role_name* **{profile1** *profile_name* **[profile2** *profile_name***] [profile3** *profile_name***]}**

no unp user-role *role_name* **[profile1] [profile2] [profile3]**

Syntax Definitions

role_name	The name of a user-defined role.
profile_name	The name of an existing UNP profile.

Defaults

By default, the profile condition is not configured for a user-defined role.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the profile name as a condition for the specified user-defined role.
- If the user-defined role name specified with this command does not exist, the switch will automatically create the role name and associate the profile with that name.
- The profile name specified with this command must already exist in the switch configuration.

Examples

```
-> unp user-role role1 profile1 unp1
-> unp user-role role2 profile1 unp1 profile2 unp2
-> unp user-role role3 profile1 unp1 profile2 unp2 profile3 unp3
-> no unp user-role role1 profile1
-> no unp user-role role2 profile1 profile2
-> no unp user-role role3 profile3
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp user-role	Configures the name and precedence for a user-defined role.
unp user-role policy-list	Assigns a QoS policy list to a user-defined role.
show unp user-role	Displays the user-defined role configuration for the switch.

MIB Objects

```
alaDaUNPUserRoleTable
  alaDaUNPUserRoleName
  alaDaUNPUserRoleProfile1
  alaDaUNPUserRoleProfile2
  alaDaUNPUserRoleProfile3
```

unp user-role authentication-type

Defines an authentication type condition for the specified user-defined role name.

unp user-role *role_name* **authentication-type {none | mac [fail] | 802.1x [fail]}**

no unp user-role *role_name* **authentication-type**

Syntax Definitions

role_name	The name of a user-defined role.
none	No authentication was applied to the device.
mac	The device was successfully authenticated through MAC authentication.
802.1x	The device was successfully authenticated through 802.1X authentication.
fail	Optional parameter to specify failed MAC or 802.1X authentication.

Defaults

By default, the authentication type condition is not configured for a user-defined role.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the authentication type as a condition for the specified user-defined role.
- If the user-defined role name specified with this command does not exist, the switch will automatically create the role name and associate the profile with that name.
- The optional **fail** parameter is used only in combination with the **mac** or **802.1x** parameter. When configured, the device is checked for a failed MAC or 802.1X authentication condition to determine whether or not the user role (policy list associated with the user role) is applied to the device.
- When the **fail** parameter is not specified (the default), the device is checked for a successful MAC or 802.1X authentication condition to determine whether or not the user role (policy list associated with the user role) is applied to the device.

Examples

```
-> unp user-role role1 authentication-type 8021x
-> unp user-role role1 authentication-type 8021X fail
-> unp user-role role1 authentication-type mac
-> unp user-role role1 authentication-type mac fail
-> no unp user-role role1 authentication-type
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp user-role	Configures the name and precedence for a user-defined role.
unp user-role policy-list	Assigns a QoS policy list to a user-defined role.
show unp user-role	Displays the user-defined role configuration for the switch.

MIB Objects

```
alaDaUNPUserRoleTable
  alaDaUNPUserRoleName
  alaDaUNPUserRoleAuthType
```

unp user-role cp-status-post-login

Configures the Captive Portal (CP) post login status as a condition for the specified user-defined role name.

unp user-role *role_name* **cp-status-post-login**

no unp user-role *role_name* **cp-status-post-login**

Syntax Definitions

role_name	The name of an existing user-defined role.

Defaults

By default, the CP post login status condition is not configured for a user-defined role.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the CP post login status as a condition for the specified user-defined role.
- When this condition is active for a user-defined role, the switch will check to see if a device is in a CP post login state before applying the QoS policy list associated with the user-defined role.

Examples

```
-> unp user-role role1 cp-status-post-login
-> no unp user-role role1 cp-status-post-login
```

Release History

Release 8.1.1; command was introduced.

Related Commands

unp user-role	Configures the name and precedence for a user-defined role.
unp user-role policy-list	Assigns a QoS policy list to a user-defined role.
show unp user-role	Displays the user-defined role configuration for the switch.

MIB Objects

```
alaDaUNPUserRoleTable
  alaDaUNPUserRoleName
  alaDaUNPUserRolePostLoginStatus
```

unp restricted-role policy-list

Assigns an explicit QoS policy list to an implicit restricted role. When the switch assigns a user device to one of the restricted role states (unauthorized, Quarantine Manager, or Captive Portal pre-login), the explicit QoS policy list is applied instead of the built-in policy list associated with the restricted role.

unp restricted-role {unauthorized | qmr | cp-prelogin} policy-list *list_name*

no unp restricted-role {unauthorized | qmr | cp-prelogin} policy-list

Syntax Definitions

list_name	The name of an existing QoS policy list.
unauthorized	Applies the explicit policy list to unauthorized devices.
qmr	Applies the explicit policy list to quarantined devices. *Supported only on OmniSwitch 6860 and OmniSwitch 6865.*
cp-prelogin	Applies the explicit policy list to devices in a Captive Portal pre-login state. *Not supported on OmniSwitch 6900.*

Defaults

By default, the built-in policy list associated with the restricted role state.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the explicit QoS policy list assignment.
- An explicit QoS policy list overrides the built-in policy list associated with the restricted role state.
- When the explicit policy list assignment is removed, the switch reverts back to using the built-in policy list associated with the restricted role state.

Examples

```
-> unp restricted-role unauthorized policy-list unauth1
-> unp restricted-role qmr policy-list quarantined1
-> unp restricted-role cp-prelogin policy-list cplogin1
-> no unp restricted-role unauthorized
-> no unp restricted-role qmr
-> no unp restricted-role cp-prelogin
```

Release History

Release 8.1.1; command was introduced.

Related Commands

policy list	Configures a QoS policy list.
show unp restricted-role	Displays the UNP restricted role policy list configuration.

MIB Objects

```
alaDaUNPRstrctedRoleTable
  alaDaUNPRstrctedRoleType
  alaDaUNPRstrctedRolePolicyList
```

captive-portal mode

Configures the Captive Portal mode of operation.

captive-portal mode {internal | internal dhcp [ip-lease-time *seconds***] [ip-renew-time** *seconds***] [ip-rebinding-time** *seconds***] | external}**

no captive-portal mode internal

Syntax Definitions

internal	Internal Captive Portal (Web server is on the switch. A VLAN change requires a port bounce).
internal dhcp	Internal DHCP Captive Portal (Web server is on the switch. IP address from Captive Portal subnet is leased to the client; VLAN change does not require a port bounce).
ip-lease-time *seconds*	The amount of time an IP address is leased to a client. The valid range is 20–120 seconds.
ip-renew-time *seconds*	The amount of time until a client with a leased IP address attempts to renew the leased IP address.
ip-rebinding-time *seconds*	The amount of time until a client attempts to obtain a new leased IP address (occurs when renew attempts fail).
external	Not supported; an external Captive Portal operation is provided through the OmniSwitch Bring Your Own Device (BYOD) solution.

Defaults

By default, the mode is set to internal Captive Portal. When the internal DHCP Captive Portal mode is selected without specifying any optional parameter values, the following default values are set:

parameter	default
ip-lease-time	30 seconds
ip-renew-time	15 seconds
ip-rebinding-time	26 seconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to revert the Captive Portal mode back to the default internal mode (no internal DHCP functionality).
- Only the internal and internal DHCP Captive Portal modes (Web server on the switch) are configurable for the switch. An external Captive Portal operation is provided through interaction with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch BYOD solution.

- When a device is classified into a UNP profile that has the Captive Portal authentication attribute enabled, the device is placed into a Captive Portal pre-login state. The Captive Portal mode determines how a device in the pre-login state obtains an IP address, the necessary DNS information, and whether a port bounce is required after a VLAN change.
  - If the internal Captive Portal mode (the default) is active, the device can directly contact a DHCP server to get an IP address and DNS information. A port bounce action is required if the initial VLAN assignment for the device is changed.
  - If the internal DHCP Captive Portal mode is active, the switch provides basic DHCP functionality to assign the device an IP address with a short-term lease from the Captive Portal subnet (10.123.0.0) and provide the necessary DNS information. A port bounce action is not required if the initial VLAN assignment for the device is changed.
- Consider the following when changing the internal DHCP parameter values:
  - The **ip-renew-time** is 50% of the **ip-lease-time**.
  - The **ip-rebinding-time** is 87.5% of the **ip-lease-time**.
  - When only the **ip-lease-time** is changed, the **ip-renew-time** and **ip-rebinding-time** are automatically recalculated based on the noted percentages.
  - Make sure the **ip-renew-time** specified is less than the **ip-rebinding-time**.
  - Make sure the **ip-rebinding-time** specified falls between the **ip-renew-time** and **ip-lease-time**.

Examples

```
-> captive-portal mode internal-dhcp
-> captive-portal mode internal-dhcp ip-least-time 120
-> captive-portal mode internal
-> no captive-portal mode internal
```

Release History

Release 8.5R4; command was introduced.

Related Commands

show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalMode
   alaDaCPortalDHCPLeaseTime
   alaDaCPortalDHCPRenewTime
   alaDaCPortalDHCPRebindingTime
```

captive-portal name

Configures an IP address or Fully Qualified Domain Name (FQDN) as a redirect URL to use for Captive Portal.

captive-portal name {*ip_address* | *domain_name***}**

no captive-portal name

Syntax Definitions

ip_address	The IPv4 network address (e.g., 171.15.0.0) to which HTTP traffic is redirected.
domain_name	An FQDN (up to 32 characters) to which HTTP traffic is redirected.

Defaults

By default, the Captive Portal redirect name is set to “captive-portal.com”.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to revert the URL name back to the default “captive-portal.com”.
- Use this command to change the Captive Portal redirect URL name to match the common name (cn) used by the public certificate on the switch. Matching these two names prevents a certificate warning message caused when these names do not match.

Note. Do not preface the redirect URL domain name with **https://**; the switch automatically adds **https://** to the beginning of the domain name.

- When a device is classified into a UNP profile that has the Captive Portal authentication attribute enabled, the device is placed into a Captive Portal pre-login state. In this state, the device can contact a DHCP server to get an IP address and get the DNS server address.
- Initial HTTP requests received from a user device are responded to with the Captive Portal redirect name. The user device contacts the DNS server to resolve the redirect name and receives the Captive Portal IP address. Requests are then sent to the Captive Portal IP address that is mapped internally to the OmniSwitch web server, which then presents login Web pages to the user device.
- Make sure the DNS server configuration reflects the same Captive Portal name and IP address that is configured for the OmniSwitch.

Examples

```
-> captive-portal name cert-name
-> captive-portal name “20.2.2.1”
-> no captive-portal name
```

Release History

Release 8.1.1; command was introduced.

Related Commands

captive-portal ip-address	Configures the internal Captive Portal IP address for the switch.
show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalRedirectUrlName
```

captive-portal ip-address

Configures the internal Captive Portal IP address for the switch.

captive-portal ip-address *ip_address*

Syntax Definitions

ip_address	IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).

Defaults

By default, the internal Captive Portal IP address is set to 10.123.0.1.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the default 10.123.0.0 subnet is already in use, then use this command to change the Captive Portal IP address to another 10.x.0.0 subnet (only the second octet of the Captive Portal IP address can be changed).
- When a device is classified into a UNP profile that has the Captive Portal authentication attribute enabled, the device is placed into a Captive Portal pre-login role. In this state, the device can contact a DHCP server to get an IP address and get the DNS server address.
- Initial HTTP requests received from a user device are responded to with the Captive Portal redirect name. The user device contacts the DNS server to resolve the redirect URL name and receives the Captive Portal IP address. Requests are then sent to the Captive Portal IP address that is mapped internally to the OmniSwitch web server, which then presents login web pages to the user device.
- Make sure the DNS server configuration reflects the same Captive Portal name and IP address that is configured for the OmniSwitch.

Examples

```
-> captive-portal ip-address 10.255.0.20
```

Release History

Release 8.1.1; command was introduced.

Related Commands

captive-portal name	Configures the name of the redirect URL that is used for accessing a public certificate.
show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalIpAddress
```

captive-portal success-redirect-url

Configures the URL of a specific site to which a user is redirected after a successful Captive Portal authentication.

captive-portal success-redirect-url *redirect_url*

no captive-portal success-redirect-url

Syntax Definitions

redirect_url	The redirect URL (up to 63 characters).

Defaults

By default, no success redirect URL is configured.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to remove the success redirect URL from the Captive Portal global configuration.

Examples

```
-> captive-portal success-redirect-url http://server-1.com/pass.html
-> no captive-portal success-redirect-url
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalSuccRedirectUrl
```

captive-portal proxy-server-port

Configures the proxy server port to use for Captive Portal.

captive-portal proxy-server-port *proxy_port*

no captive-portal proxy-server-port

Syntax Definitions

proxy_port	The HTTP proxy port number. The valid range is 1024–49151.

Defaults

By default, the proxy server port number is set to 8080.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to set the proxy port number back to the default (8080).
- This command overwrites the existing proxy port number for the switch.
- The proxy port number only requires changing if the proxy port used is not 80 or 8080.

Examples

```
-> captive-portal proxy-server-port 1200
-> no captive-portal proxy-server-port
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalProxyPort
```

captive-portal retry-count

Configures the number of times a device can try to login before Captive Portal determines that authentication for that device has failed.

captive-portal retry-count *retries*

Syntax Definitions

retries	The number of login attempts allowed. The valid range is 1–99.

Defaults

By default, the retry count is set to 3.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

No access page is sent to devices that exceed the number of login retries allowed.

Examples

```
-> captive-portal retry-count 5
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalRetryCnt
```

captive-portal authentication-pass

Configures a global authentication pass policy. This type of policy is applied to all devices successfully authenticated through the Captive Portal process. Each policy can specify a QoS policy list and UNP profile name to assign to the authenticated devices.

captive-portal authentication-pass {policy-list *list_name* **| profile** *profile_name* **| profile-change {enable | disable}}**

no captive-portal authentication-pass {policy-list | profile}

Syntax Definitions

list_name	The name of a QoS policy list to apply to the authenticated user device.
profile_name	The name of an existing UNP profile.
enable	Enables the profile change operation. Authenticated devices are assigned to the specified profile name.
disable	Disables the profile change operation. Authenticated devices are not assigned to a new profile.

Defaults

By default, no policy list name or UNP profile name is specified for the global Captive Portal configuration.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the Captive Portal authentication pass policy from the global Captive Portal configuration.
- When the **profile-change** parameter is enabled, the profile initially assigned to the Captive Portal users is changed to the profile derived through successful Captive Portal authentication. The QoS policy list associated with the new profile is applied to the authenticated users.
- When a profile change occurs, the new profile may assign a different VLAN to the authenticated device. This new VLAN assignment is functional only after a port bounce or pause timer operation is completed. Existing Bring Your Own Device (BYOD) global commands are leveraged to configure the port bounce and pause timer values.
- If the new UNP profile assigned also has Captive Portal authentication enabled, the process is not started again. The results from the initial Captive Portal authentication process are used instead.
- When the **profile-change** parameter is disabled, the QoS policy list name returned from the RADIUS server or the list name specified with this command is applied instead.
- The QoS policy list to apply to Captive Portal authenticated devices is derived through one of the following methods:
  - The policy list name returned from the RADIUS server.

  - The policy list name specified with this command for the global Captive Portal configuration.
  - The policy list name associated with the UNP profile returned from the RADIUS server.
  - The policy list name associated with the UNP profile specified with this command for the global Captive Portal configuration.

- A policy list name or a UNP profile name returned from the RADIUS server takes precedence over the policy list name or UNP profile name configured through this command.

Examples

```
-> captive-portal authentication-pass policy-list list1
-> captive-portal authentication-pass profile unp1-vlan profile-change enable
-> captive-portal authentication-pass profile-change disable
-> no captive-portal authentication-pass policy-list
-> no captive-portal authentication-pass profile
```

Release History

Release 8.1.1; command was introduced.
Release 8.2.1; **edge-profile** and **edge-profile-change** parameters added.
Release 8.3.1; **edge-profile** and **edge-profile-change** parameters changed to **profile** and **profile-change**.

Related Commands

captive-portal authentication-pass domain	Configures a domain specific authentication pass policy to determine the QoS policy list or UNP profile name to apply to authenticated devices. This type of policy overrides the global Captive Portal configuration.
show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalPolicyListName
   alaDaCPortalUNPProfile
   alaDaCPortalUNPProfileChange
```

captive-portal authentication-pass domain

Configures a domain specific authentication pass policy. This type of policy is applied to all devices within the specified domain that were successfully authenticated through the Captive Portal process.

captive-portal authentication-pass realm {prefix | suffix} domain *domain_name* **{policy-list** *list_name* **| profile** *profile_name* **| profile-change {enable | disable}}**

no captive-portal authentication-pass [realm {prefix | suffix} domain *domain_name***]**

Syntax Definitions

prefix	Specifies a prefix domain name (for example, *domain_name*/user).
suffix	Specifies a suffix domain name (for example, user@*domain_name*)
domain_name	The domain name for the user device.
list_name	The name of a QoS policy list to apply to the authenticated user device.
profile_name	The name of an existing UNP profile.
enable	Enables the profile change operation. Authenticated devices are assigned to the specified profile name.
disable	Disables the profile change operation. Authenticated devices are not assigned to a new profile.

Defaults

By default, no domain specific authentication pass policy is configured for the Captive Portal process.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the domain specific authentication pass policy from the Captive Portal configuration.
- Use the **realm prefix domain** or **realm suffix domain** parameter to apply the authentication policy list or UNP profile based on the domain name of the Captive Portal authenticated user device.
- If the **profile-change** parameter is enabled, the profile initially assigned to the Captive Portal user is changed to the profile derived through successful Captive Portal authentication. The QoS policy list associated with the new profile is then applied to the authenticated users.
- When a profile change occurs, the new profile may assign a different VLAN to the authenticated device. This new VLAN assignment is functional only after a port bounce or pause timer operation is completed. Existing Bring Your Own Device (BYOD) global commands are leveraged to configure the port bounce and pause timer values.
- If the new profile assigned to the user also has Captive Portal authentication enabled, the process is not started again. The results from the initial Captive Portal authentication process are used instead.

- If the **profile-change** parameter is disabled, then the QoS policy list name returned from the RADIUS server or the list name specified through the global (non-domain specific) Captive Portal configuration is applied.
- The QoS policy list to apply to Captive Portal authenticated devices is derived through one of the following methods:
  - The policy list name returned from the RADIUS server.
  - The policy list name specified with this command or through the global Captive Portal configuration.
  - The policy list name associated with the UNP profile returned from the RADIUS server.
  - The policy list name associated with the UNP profile specified with this command or through the global Captive Portal configuration.
- A policy list name or a UNP profile name returned from the RADIUS server takes precedence over the policy list name or UNP profile name configured through this command.

Examples

```
-> captive-portal authentication-pass realm prefix domain asia-pacific policy-list
list2
-> captive-portal authentication-pass realm suffix domain north-america profile
unp2 profile-change enable
-> no captive-portal authentication-pass realm suffix domain north-america
```

Release History

Release 8.1.1; command was introduced.
Release 8.2.1; **edge-profile** and **edge-profile-change** parameters added.
Release 8.3.1; **edge-profile** and **edge-profile-change** parameters changed to **profile** and **profile-change**.

Related Commands

captive-portal authentication-pass	Configures a global authentication pass policy. This type of policy is applied to all devices successfully authenticated through the Captive Portal process.
show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalAuthPassTable
   alaDaCPortalAuthDomainName
   alaDaCPortalAuthRealm
   alaDaCPortalAuthPolicyListName
   alaDaCPortalAuthRowStatus
   alaDaCPortalAuthUNPProfile
   alaDaCPortalAuthUNPProfileChange
```

captive-portal-profile

Configures a Captive Portal profile that is assigned to a UNP profile. This type of profile defines Captive Portal configuration options that are applied to devices classified into the assigned UNP profile. This command page describes the base command (**captive-portal-profile** *profile_name*) along with the other command keywords that are used to configure profile attributes.

captive-portal-profile *profile_name*
[aaa-profile *aaa_profile_name***]**
[success-redirect-url *redirect_url***]**
[retry-count *retries***]**
[authentication-pass [realm {prefix | suffix} domain *domain_name***] {policy-list** *list_name* **| profile** *profile_name* **| profile-change {enable | disable}}]**

no captive-portal-profile *profile_name*

Syntax Definitions

profile_name	The name to assign to the Captive Portal profile (up to 32 characters).
aaa_profile_name	The name of an authentication, authorization, and accounting (AAA) profile to associate with the Captive Portal profile.
redirect_url	A URL (up to 63 characters) to which user devices are redirected after successful Captive Portal authentication.
retries	The number of login attempts allowed. The range is 1–99.
realm prefix	Specifies a prefix domain name (for example, *domain_name*/user).
realm suffix	Specifies a suffix domain name (for example, user@*domain_name*).
domain_name	The domain name for the user device.
list_name	The name of a QoS policy list to apply to the authenticated user device.
profile_name	The name of an existing UNP profile.
enable	Enables the profile change operation. Authenticated devices are assigned to the specified profile name.
disable	Disables the profile change operation. Authenticated devices are not assigned to a new profile.

Defaults

parameter	default
aaa_profile_name	none
redirect_url	none
retries	3
realm prefix | suffix	none
domain_name	none
list_name	none
profile_name	none
enable | disable	disabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the Captive Portal profile from the switch configuration.
- Creating a Captive Portal profile name with the base command (**captive-portal-profile** *profile_name*) is not required to configure a profile attribute value. If the profile name does not exist, the switch will automatically create the name specified when the attribute is configured. For example, the **unp captive-portal-profile cp-prof1 retry-count 5** command will create the "cp-prof1" profile if it does not already exist in the switch configuration.
- When a Captive Portal profile is applied to a UNP profile, the parameter values defined in the profile override the global Captive Portal parameter values configured for the switch.
- A Captive Portal profile is applied only when Captive Portal authentication is enabled for the UNP profile. If there is no Captive Portal profile associated with a UNP profile, then the global Captive Portal configuration is applied.
- Assigning an AAA profile to a Captive Portal profile defines specific AAA configuration options (such as RADIUS servers and RADIUS client attributes) that are used for Captive Portal authentication. If there is no AAA profile assigned, then the global AAA configuration is used.
- AAA profiles are configured using the **aaa profile** command. See the "AAA Commands" chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide* for more information.

Examples

```
-> captive-portal-profile cp-p1
-> captive-portal-profile cp-p1 aaa-profile aaa_p1
-> captive-portal-profile cp-p1 authentication-pass realm prefix domain asia-
pacific policy-list list1
-> no captive-portal-profile cp-p1 aaa-profile aaa_p1
-> no captive-portal-profile cp-p1

-> captive-portal-profile cp-p2 retry-count 5
-> captive-portal-profile cp-p2 authentication-pass profile ep-1
-> captive-portal-profile cp-p2 authentication-pass profile-change enable
```

```
-> captive-portal-profile cp-p2 success-redirect-url http://server-1.com/pass.html
-> captive-portal-profile cp-p2 authentication-pass profile-change disable
-> no captive-portal-profile cp-p2 authentication-pass profile
-> no captive-portal-profile cp-p2
```

Release History

Release 8.1.1; command was introduced.
Release 8.2.1; **edge-profile** and **edge-profile-change** parameters added.
Release 8.3.1; **edge-profile** and **edge-profile-change** parameters changed to **profile** and **profile-change**.

Related Commands

unp profile captive-portal-profile	Assigns a Captive Portal profile to a UNP profile.
aaa profile	Configures an AAA configuration profile.
show captive-portal profile-names	Displays the Captive Portal profile configuration for the switch.

MIB Objects

```
 alaDaCPortalProfTable
   alaDaCPortalProfName
   alaDaCPortalProfSuccRedirectUrl
   alaDaCPortalProfRetryCnt
   alaDaCPortalProfAuthPolicyListName
   alaDaCPortalProfAaaProf
   alaDaCPortalProfUNPProfile
   alaDaCPortalProfUNPProfileChange
alaDaCPortalProfDomainTable
   alaDaCPortalProfDomainAuthDomainName
   alaDaCPortalProfDomainAuthPolicyListName
   alaDaCPortalProfDomainAuthRealm
   alaDaCPortalProfDomainUNPProfile
   alaDaCPortalProfDomainUNPProfileChange
```

captive-portal customization

Enables or disables the use of custom Web pages for Captive Portal authentication. When customization is enabled, Captive Portal presents Web pages stored in the “/flash/switch/captive_portal/custom_files/” directory on the switch. When customization is disabled, Captive Portal presents Web pages stored in the “/flash/switch/captive_portal/release_files/” directory on the switch.

captive-portal customization {enable | disable}

Syntax Definitions

enable	Displays custom web pages for Captive Portal authentication.
disable	Displays default web pages for Captive Portal authentication.

Defaults

By default, the web pages provided on the switch are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To create custom Web pages, create a folder in the same path as the “release_files” folder and name the new folder “custom_files” (for example “/flash/switch/captive_portal/custom_files/”). Next, copy the “assets” and “templates” folders found under “/flash/switch/captive_portal/release_files/” to the “custom_files” folder. Modify the contents in the copied folders to create custom Web pages.
- The “release_files” folder is overwritten each time the switch reboots, so ***DO NOT*** modify the files in this folder for custom use.
- The folders "assets" and "templates" under the /flash/switch/captive_portal/custom_files/ directory are used to create and display Web pages to Captive Portal users when the switch reboots or at runtime when Captive Portal customization is enabled for the switch, if the “custom_files” folder exists.
- Anything in the custom "assets" folder is statically served by the internal Web server on the switch whenever they are requested. These pages are typically **.css** files, javascript files, or the acceptable use policy and are linked to files in the custom "templates" folder.
- The custom "templates" folder contains the Web pages that are dynamically served to users depending on the Captive Portal state of each user. The file names in this folder must not be changed. The login form field names and form action in these pages must not be changed. The variables in these pages, as denoted by "<?=$(name)?>”, are substituted in place by the internal Web server.

Examples

```
-> captive-portal customization enable
-> captive-portal customization disable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalCustomization
```

show captive-portal configuration

Displays the global Captive Portal parameter settings configured for the switch.

show captive-portal configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Currently only the internal Captive Portal mode (Web server on the switch) is configurable for the switch. An external Captive Portal operation is provided through interaction with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch BYOD solution.
- The parameter values configured and applied through a Captive Portal profile override any values set through the global Captive Portal configuration. A Captive Portal profile is associated with a UNP profile and is applied to devices classified into that profile.

Examples

```
-> show captive-portal configuration
Captive Portal Global Configuration:

  Captive Portal Mode                  = Internal
  DHCP Parameters:
     DHCP Lease Time     = 30
     DHCP Renew Time     = 15
     DHCP Rebinding Time = 26
  Captive Portal IP address            = 10.123.0.1
  Captive Portal Redirect String       = captive-portal.com
  Captive Portal Success Redirect URL  =
  Captive Portal Proxy Server Port     = 8080
  Captive Portal Retry Count           = 3
  Captive Portal Global Auth Policy List=
  Captive Portal Page Customization    = Disable
  Captive Portal Profile Name          =
  Captive Portal Profile Change        = Disable
  Domain Specific Policy Lists:
        Domain       | Realm |     Policy List     |   Profile Name      | Profile
                     |       |                     |                     | Change
---------------------|-------|---------------------|---------------------|---------
na01                 |Suffix |qos-bw1              |unp1-vlan            |Enable
na02                 |Prefix |qos-bw2              |unp2-vlan            |Enable
```

output definitions

Captive Portal Mode	The Captive Portal mode of operation. Only the internal and internal DHCP modes (Web server on the OmniSwitch) are supported at this time. Configured through the **captive-portal mode** command.
DHCP Parameters:	A list of DHCP parameter values that are applied when the internal DHCP mode is active. These fields display "N/A" when the internal DHCP mode is not active. Configured through the **captive-portal mode** command.
DHCP Lease Time	The amount of time an IP address is leased to a DHCP client.
DHCP Renew Time	The amount of time, in seconds, until an attempt is made to renew the leased IP address (50% of the DHCP Lease Time).
DHCP Rebinding Time	The amount of time until an attempt is made to obtain a new IP leased address (87.5% of the DHCP Lease Time).
Captive Portal IP address	The internal Captive Portal IP address for the switch. Configured through the **captive-portal ip-address** command.
Captive Portal Redirect String	The name of the redirect URL that is used for accessing a public certificate. Configured through the **captive-portal name** command.
Captive Portal Success Redirect URL	The URL of a specific site to which a user is redirected after a successful Captive Portal authentication. Configured through the **captive-portal success-redirect-url** command.
Captive Portal Proxy Server Port	The proxy server port to use for Captive Portal. Configured through the **captive-portal proxy-server-port** command.
Captive Portal Retry Count	The number of times a device can try to login before Captive Portal determines that authentication for that device has failed. Configured through the **captive-portal retry-count** command.
Captive Portal Global Auth Policy List	The name of a QoS policy list for the global Captive Portal configuration. The specified list is applied to each device that passes Captive Portal authentication. Configured through the **captive-portal authentication-pass** command.
Captive Portal Page Customization	Whether or not (**Enable** or **Disable**) customized Captive Portal pages are presented to the user.
Captive Portal Profile Name	The name of a UNP profile for the global Captive Portal configuration. The specified profile is only applied to Captive Portal authenticated devices when the Captive Portal profile change option is enabled. Configured through the **captive-portal authentication-pass** command.
Captive Portal Profile Change	The status of profile change (**Enable** or **Disable**). When enabled, the profile initially assigned to the Captive Portal user is changed to the profile specified through the Captive Portal profile name option. Configured through the **captive-portal authentication-pass** command.
Domain Specific Policy Lists:	A list of Captive Portal domain specific policies. The policy list is applied when the domain for a Captive Portal authenticated device matches the domain criteria associated with the list. Domain specific policies take precedence over the global Captive Portal settings.
Domain	The domain name associated with a domain specific policy. Configured through the **captive-portal authentication-pass domain** command.

output definitions

Realm	The realm of the domain name (**prefix** or **suffix**) associated with a domain specific policy. The realm identifies the domain name as a prefix (*domain-name*/user) or as a suffix (user@*domain-name*). Configured through the **captive-portal authentication-pass domain** command.
Policy List	The name of the QoS policy list that is applied when the domain of a Captive Portal authenticated user device matches the domain criteria associated with the list name. Configured through the **captive-portal authentication-pass domain** command.
Profile Name	The name of the UNP profile that is applied when the domain of a Captive Portal authenticated user device matches the domain criteria associated with the profile name. Configured through the **captive-portal authentication-pass domain** command.
Profile Change	The status of profile change (**Enable** or **Disable**) for the associated domain name. When enabled, the initial profile assigned to the Captive Portal device is changed to the profile specified through the profile change option associated with the domain name. Configured through the **captive-portal authentication-pass domain** command.

Release History

Release 8.1.1; command was introduced.
Release 8.5R4; DHCP Parameter fields added.

Related Commands

show captive-portal profile-names	Displays the Captive Portal profile configuration for the switch.

MIB Objects

```
alaDaCPortalGlobalConfig
   alaDaCPortalMode
   alaDaCPortalDHCPLeaseTime
   alaDaCPortalDHCPRenewTime
   alaDaCPortalDHCPRebindingTime
   alaDaCPortalIpAddress
   alaDaCPortalRedirectUrlName
   alaDaCPortalSuccRedirectUrl
   alaDaCPortalProxyPort
   alaDaCPortalRetryCnt
   alaDaCPortalPolicyListName
   alaDaCPortalCustomization
   alaDaCPortalUNPProfile
   alaDaCPortalUNPProfileChange
alaDaCPortalAuthPassTable
   alaDaCPortalAuthDomainName
   alaDaCPortalAuthRealm
   alaDaCPortalAuthPolicyListName
   alaDaCPortalAuthRowStatus
   alaDaCPortalAuthUNPProfile
   alaDaCPortalAuthUNPProfileChange
```

show captive-portal profile-names

Displays the Captive Portal profile configuration for the switch.The parameter values configured and applied through a Captive Portal profile override any values set through the global Captive Portal configuration.

show captive-portal {profile-names | profile-name *profile_name* **configuration}**

Syntax Definitions

profile-names	Displays a list of configured Captive Portal profiles.
profile-name *profile_name* **configuration**	Displays the Captive Portal parameter configuration for the specified profile name.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Currently only the internal Captive Portal mode (Web server on the switch) is configurable for the switch. An external Captive Portal operation is provided through interaction with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch BYOD solution.

Examples

```
-> show captive-portal profile-names

      Captive Portal Profile Names
---------------------------------------
1. cp1
2. cp2
3. cp3

-> show captive-portal profile-name cp1 configuration

Captive Portal Profile cp1 Configuration:
  Captive Portal Mode                  = Internal
  Captive Portal AAA Profile Name      =
  Captive Portal Success Redirect URL  =
  Captive Portal Retry Count           = 3
  Captive Portal Global Auth Policy List =
  Captive Portal Profile Name          =
  Captive Portal Profile Change        = Disable
 Domain Specific Policy Lists:
        Domain       | Realm |     Policy List     |   Profile Name      | Profile
                     |       |                     |                     | Change
---------------------|-------|---------------------|---------------------|---------
na01                 |Suffix |qos-bw1              |unp1-vlan            |Enable
na02                 |Prefix |qos-bw2              |unp2-vlan            |Enable
```

output definitions

Captive Portal Mode	The Captive Portal mode of operation. Only internal mode (Web server on the OmniSwitch) is supported at this time.
Captive Portal AAA Profile Name	The name of an authentication, authorization, and accounting (AAA) profile associated with the Captive Portal profile.
Captive Portal Success Redirect URL	The URL of a specific site to which a user is redirected after a successful Captive Portal authentication.
Captive Portal Retry Count	The number of times a device can try to login before Captive Portal determines that authentication for that device has failed.
Captive Portal Global Auth Policy List	The name of a QoS policy list for the global Captive Portal configuration. The specified list is applied to each device that passes Captive Portal authentication.
Captive Portal Profile Name	The name of a UNP profile for the global Captive Portal configuration. The specified profile is only applied to Captive Portal authenticated devices when the Captive Portal profile change option is enabled.
Captive Portal Profile Change	The status of profile change (**Enable** or **Disable**). When enabled, the profile initially assigned to the Captive Portal user is changed to the profile specified through the Captive Portal profile name option.
Domain Specific Policy Lists:	A list of Captive Portal domain specific policies. The policy list is applied when the domain for a Captive Portal authenticated device matches the domain criteria associated with the list. Domain specific policies take precedence over the global Captive Portal settings.
Domain	The domain name associated with a domain specific policy.
Realm	The realm of the domain name (**prefix** or **suffix**) associated with a domain specific policy. The realm identifies the domain name as a prefix (*domain-name*/user) or as a suffix (user@*domain-name*).
Policy List	The name of the QoS policy list that is applied when the domain of a Captive Portal authenticated user device matches the domain criteria associated with the list name.
Profile Name	The name of the UNP profile that is applied when the domain of a Captive Portal authenticated user device matches the domain criteria associated with the profile name.
Profile Change	The status of profile change (**Enable** or **Disable**) for the associated domain name. When enabled, the initial profile assigned to the Captive Portal device is changed to the profile specified through the profile change option associated with the domain name.

Release History

Release 8.1.1; command was introduced.

Related Commands

captive-portal-profile	Configures a Captive Portal profile.
show captive-portal configuration	Displays the global Captive Portal parameter settings configured for the switch

MIB Objects

```
alaDaCPortalProfTable
  alaDaCPortalProfName
  alaDaCPortalProfSuccRedirectUrl
  alaDaCPortalProfRetryCnt
  alaDaCPortalProfAuthPolicyListName
  alaDaCPortalProfAaaProf
  alaDaCPortalProfUNPProfile
  alaDaCPortalProfUNPProfileChange
```

qmr quarantine path

Specifies the URL for a remediation server. This information is used by the Quarantine Manager and Remediation (QMR) application. A quarantined user is redirected to a remediation server to correct the condition that put the user into a quarantined state.

qmr quarantine path *url*

no qmr quarantine path

Syntax Definitions

url	The URL for the QMR remediation server.

Defaults

By default, no URL is configured.

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

- Use the **no** form of the command to remove the remediation server URL from the configuration.
- Make sure to add the corresponding IP address for the remediation server to the QMR list of exception subnets, configured through the **qmr quarantine allowed-name** command.
- Configuring the URL *and* adding the server IP address to the allowed list is required to redirect quarantined MAC addresses to the remediation server.

Examples

```
-> qos quarantine path www.remediate.com
-> no quarantine path
```

Release History

Release 8.1.1; command was introduced.

Related Commands

qmr quarantine page	Configures whether or not QMR will send a “Quarantined” page to a user when a remediation server is not configured.
qmr quarantine allowed-name	Configures a list of IP addresses to which a restricted quarantined user can access.
qmr quarantine custom-proxy-port	Configures the HTTP proxy port number that is used to redirect traffic from a quarantined device.
qos quarantine mac-group	Configures the name of the Quarantine MAC address group.
show qmr	Displays the Access Guardian QMR configuration.
show quarantine mac group	Displays the contents of the QoS quarantined MAC address group.

MIB Objects

```
alaDaQMRGlobalConfig
   alaDaQMRPath
```

qmr quarantine page

Configures the QMR application to send a “Quarantined” page to a client if a remediation server is not configured. This page is used to notify the client that QMR has quarantined the client.

qmr qos quarantine page {enable | disable}

Syntax Definitions

enable	Enables the sending of a “Quarantined” page to the client.
disable	Disables the sending of a “Quarantined” page to the client.

Defaults

By default, no “Quarantined” page is sent to the client.

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

A “Quarantined” page is only sent if a remediation server path was not configured for QMR. Note that even if the remediation server is not active, QMR will not send the page as long as there is a value set for the remediation server path.

Examples

```
-> qmr quarantine page enable
-> qmr quarantine page disable
```

Release History

Release 8.1.1; command was introduced.

Related Commands

qmr quarantine path	Specifies the URL for a remediation server.
qmr quarantine allowed-name	Configures a list of IP addresses to which a restricted quarantined user can access.
qmr quarantine custom-proxy-port	Configures the HTTP proxy port number that is used to redirect traffic from a quarantined device.
qos quarantine mac-group	Configures the name of the Quarantine MAC address group.
show qmr	Displays the Access Guardian QMR configuration.
show quarantine mac group	Displays the contents of the QoS quarantined MAC address group.

MIB Objects

```
alaDaQMRGlobalConfig
   alaDaQMRPage
```

qmr quarantine allowed-name

Configures a list of IP addresses that a restricted quarantined user is allowed to access.

qmr quarantine allowed-name *name* **ip-address** *ip_address* **[ip-mask** *ip_mask***]**

no qmr quarantine allowed-name *name*

Syntax Definitions

name	Specify a name to assign to the allowed IP network address.
ip_address	An IPv4 network address (for example, 10.0.0.0, 171.15.0.0, or 196.190.254.0).
ip_mask	A valid IP address mask for the allowed IP network address (for example, 255.0.0.0 or 255.255.0.0)

Defaults

By default, no IP addresses are configured as QMR allowed addresses.

parameter	default
ip_mask	IP address class

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

- Use the **no** form of this command to remove an IP address from the allowed list.
- A maximum of three allowed IP addresses is supported.
- Make sure the IP address of the QMR remediation server is configured as an allowed IP address. A quarantined user is redirected to a remediation server to correct the condition that put the user into a quarantined state.

Examples

```
-> qmr quarantine allowed-name server2 ip-address 10.0.0.20 ip-mask 255.0.0.0
-> no qmr quarantine allowed-name server2
```

Release History

Release 8.1.1; command was introduced.

Related Commands

qmr quarantine path	Specifies the URL for a remediation server.
qmr quarantine page	Configures whether or not QMR will send a “Quarantined” page to a user when a remediation server is not configured.
qmr quarantine custom-proxy-port	Configures the HTTP proxy port number that is used to redirect traffic from a quarantined device.
qos quarantine mac-group	Configures the name of the Quarantine MAC address group.
show qmr	Displays the Access Guardian QMR configuration.
show quarantine mac group	Displays the contents of the QoS quarantined MAC address group.

MIB Objects

```
alaDaQMRAllowedTable
   alaDaQMRAllowedName
   alaDaQMRAllowedIpAddr
   alaDaQMRAllowedIpMask
```

qmr quarantine custom-proxy-port

Configures the HTTP proxy port number used in the Web browser configuration of a host device. Quarantine Manager uses this information when trapping HTTP packets from a quarantined device and redirecting traffic from the device for remediation.

qmr quarantine custom-proxy-port *proxy_port*

no qmr quarantine custom-proxy-port

Syntax Definitions

proxy_port	The HTTP proxy port number. The valid range is 1025–65535.

Defaults

By default, the redirect proxy port number is set to 8080.

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

Use the **no** form of this command to set the proxy port number back to 8080 (the default).

Examples

```
-> qmr quarantined custom-proxy-port 8887
-> no qmr quarantined custom-proxy-port
```

Release History

Release 8.1.1; command was introduced.

Related Commands

qmr quarantine path	Specifies the URL for a remediation server.
qmr quarantine page	Configures whether or not QMR will send a “Quarantined” page to a user when a remediation server is not configured.
qmr quarantine allowed-name	Configures a list of IP addresses to which a restricted quarantined user can access.
qos quarantine mac-group	Configures the name of the Quarantine MAC address group.
show qmr	Displays the Access Guardian QMR configuration.
show quarantine mac group	Displays the contents of the QoS quarantined MAC address group.

MIB Objects

```
alaDaQMRGlobalConfig
  alaDaQMRCustomHttpProxyPort
```

show qmr

Displays the Quarantine Manager and Remediation (QMR) configuration for the switch.

show qmr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

QMR is an OmniSwitch application that interacts with the OmniVista Quarantine Manager (OVQM) application to restrict the network access of quarantined clients and provide a remediation path for such clients to regain their network access. This command displays the OmniSwitch QMR configuration.

Examples

```
-> show qmr

Quarantine Mac Group Name    : Quarantine,
Allowed IP Subnets           : IT-HD 135.254.1.10 /255.255.255.248,
                               oss-lan 10.1.1.0 /255.255.255.0,
                               rem-ser 135.254.200.0 /255.255.255.0,
Custom Proxy port            : 8888,
Quarantine Path              : www.remediation-server.alu.com,
Quarantine Page              : enabled,
```

output definitions

Quarantine MAC Group Name	The name of the QoS Quarantine MAC address group. Configured through the **qos quarantine mac-group** command.
Allowed IP Subnets	A list of IP network addresses that devices can still access while in a quarantined state. Configured through the **qmr quarantine allowed-name** command.
Custom Proxy port	The HTTP proxy port number used for redirection of HTTP traffic from quarantined devices. Configured through the **qmr quarantine custom-proxy-port** command.

output definitions

Quarantine Path	The URL of a remediation server to which a device is redirected when the device is quarantined. Configured through the **qmr quarantine path** command.
Quarantine Page	Whether or not QMR sends a “Quarantined” page notification to a quarantined user when there is no remediation server configuration. Configured through the **qmr quarantine page** command.

Release History

Release 8.1.1; command was introduced.

Related Commands

show quarantine mac group	Displays the contents of the QoS Quarantine MAC address group.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigQuarantineMacGroupName
alaDaQMRAllowedTable
   alaDaQMRAllowedName
   alaDaQMRAllowedIpAddr
   alaDaQMRAllowedIpMask
alaDaQMRGlobalConfig
   alaDaQMRCustomHttpProxyPort
   alaDaQMRPath
   alaDaQMRPage
```

show quarantine mac group

Displays the contents of the QoS Quarantine MAC address group.

show quarantine mac group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865

Usage Guidelines

The QoS MAC address group contains the MAC addresses of clients that the OmniVista Quarantine Manager (OVQM) application has quarantined. This command displays the quarantined MAC addresses that belong to this group.

Examples

```
-> show quarantine mac group

Group Name    : Quarantine,
Number of MACs quarantined    : 11,
00:00:00:11:11:1b,
00:00:00:11:11:1a,
00:00:00:11:11:19,
00:00:00:11:11:18,
00:00:00:11:11:17,
00:00:00:11:11:16,
00:00:00:11:11:15,
00:00:00:11:11:14,
00:00:00:11:11:13,
00:00:00:11:11:12,
00:00:00:11:11:11,
```

Release History

Release 8.1.1; command was introduced.

Related Commands

qos quarantine mac-group	Configures the name of the QoS Quarantine MAC address group.

MIB Objects

N/A

zeroconf mdns admin-state

Enables or disables the Multicast DNS (mDNS) relay on the switch.

zeroconf mdns admin-state {enable | disable}

Syntax Definitions

enable	Enables the mDNS relay on the switch.
disable	Disables the mDNS relay on the switch.

Defaults

The mDNS relay feature is disabled by default.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Apple device use mDNS (multicast DNS) as the underlying protocol for Bonjour exchanges.
- The mDNS packets will be handled in the conventional way on disabling the mDNS relay on the switch.

Example

```
-> zeroconf mdns admin-state enable
-> zeroconf mdns admin-state disable
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf ssdp admin-state	Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfMdnsAdminStatus
```

zeroconf ssdp admin-state

Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch. SSDP relay enables the OmniSwitch to allow non-Apple devices to discover services with minimal configuration by the administrator.

zeroconf ssdp admin-state {enable | disable}

Syntax Definitions

enable	Enables the SSDP relay on the switch.
disable	Disables the SSDP relay on the switch.

Defaults

The SSDP relay feature is disabled by default.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The Digital Living Network Alliance (DLNA) uses Universal Plug and Play (UPnP) for media management, discovery, and control. DLNA/UPnP uses SSDP to discover services, similar to how Bonjour uses mDNS for the same. All the SSDP packets coming in on an OmniSwitch are intercepted and tunneled through the GRE tunnel to the WLAN controller (acting as a gateway).
- When SSDP relay is disabled on the switch, SSDP packets are handled in the same manner as conventional packets.

Example

```
-> zeroconf ssdp admin-state enable
-> zeroconf ssdp admin-state disable
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf mdns admin-state	Enables or disables the Multicast DNS (mDNS) relay on the switch.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfSsdpAdminStatus
```

zeroconf mode

Configures the mode of the SSDP or MDNS packet processing.

zeroconf mode [tunnel [type standard] | gateway | responder]

Syntax Definitions

tunnel	This is Aruba mode. The packets are sent to the responder through the configured GRE tunnel with protocol value of 0x0. The tunnel mode is configured on the edge switch.
tunnel type standard	The packets are sent to the responder through the configured GRE tunnel with protocol value of 0x6558.
gateway	The received packets are forwarded to all the VLANs in the gateway VLAN list. The gateway mode is configured on the gateway switch.
responder	This is responder mode. The responder mode is configured on the core switch. Responder mode is not supported on an OmniSwitch 9900.

Defaults

The tunnel mode (Aruba mode) is enabled by default.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- In tunnel mode (both Aruba and Standard), the responder IP address must be configured to tunnel the mDNS or SSDP packets. The operational status will be DOWN until the responder IP address is configured.
- In tunnel mode (both Aruba and Standard) or responder mode, the mDNS and SSDP packets are processed only when the Loopback0 IP address is configured, which is considered as the source IP address for the tunneled packets. Use the **ip interface** command to configure the interface address.
- In responder mode, the tunnel for each edge switch must be configured manually.
- In responder mode if there is no service rules configured, the responder switch will learn all the service but will not process any query received from the mDNS or SSDP client.
- The switch can operate in only one mode at a time.

Example

```
-> zeroconf mode gateway
-> zeroconf mode tunnel
-> zeroconf mode responder
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf mdns admin-state	Enables or disables the Multicast DNS (mDNS) relay on the switch.
zeroconf ssdp admin-state	Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.
zeroconf responder-ip	Configures the IP address of the tunnel endpoint (zero configuration responder).
zeroconf gateway-vlan-list	Adds or deletes a VLAN from the gateway VLAN list
zeroconf access-vlan-list	Adds or deletes a VLAN from the access VLAN list.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfMode
   alaZeroConfTunnelMode
```

zeroconf responder-ip

Configures the IP address of the tunnel endpoint (zero configuration responder) on the edge switch.

zeroconf responder-ip *ip_address*

no zeroconf responder-ip *ip_address*

Syntax Definitions

ip_address	The IPv4 address of the zero configuration responder.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Only IPv4 address can be configured as a responder IP address.
- In gateway mode, the responder IP address must not be configured.
- In tunnel mode, the responder IP address must be configured to tunnel the mDNS or SSDP packets. The operational status will be DOWN until the responder IP address is configured.
- To remove the responder IP address configuration, use the **no** form of the command.

Example

```
-> zeroconf responder-ip 10.0.0.1
-> no zeroconf responder-ip 10.0.0.1
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf mdns admin-state	Enables or disables the Multicast DNS (mDNS) relay on the switch.
zeroconf ssdp admin-state	Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.
zeroconf mode	Configures the mode of the SSDP or MDNS packet processing.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfResponderIpAddr
   alaZeroConfResponderIpAddressType
```

zeroconf gateway-vlan-list

Adds or deletes a VLAN from the gateway VLAN list.

zeroconf gateway-vlan-list *vlan_id1...vlan_idn*

no zeroconf gateway-vlan-list *vlan_id1...vlan_idn*

Syntax Definitions

vlan_id	The existing VLAN ID to be added or deleted from the gateway VLAN list. The valid range is 1-4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The gateway VLAN list can be configured only in the gateway mode.
- A maximum of 10 gateway VLANs is supported.
- To remove a VLAN from the gateway VLAN list, use the **no** form of the command.

Example

```
-> zeroconf gateway-vlan-list 1 2 4
-> no zeroconf gateway-vlan-list 4
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfGatewayVlanTable
   alaZeroConfGatewayVlanEntry
```

zeroconf access-vlan-list

Adds or deletes a VLAN from the access VLAN list.

zeroconf access-vlan-list *vlan_id1...vlan_idn*

no zeroconf access-vlan-list *vlan_id1...vlan_idn*

Syntax Definitions

vlan_id	The existing VLAN ID to be added or deleted from the access VLAN list. The valid range is 1-4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The access VLAN list must be configured when the tunnel mode use GRE tunnel type standard.
- The query packets from the responder is sent to the VLANs configured in the access VLAN list.
- A maximum of 16 access VLANs is supported.
- To remove a VLAN from the access VLAN list, use the **no** form of the command.

Example

```
-> zeroconf access-vlan-list 6 7 9
-> no zeroconf access-vlan-list 7
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfAccessVlanTable
   alaZeroConfAccessVlanEntry
```

zeroconf server-policy

Configures the server policy.

zeroconf server-policy *policy_name* **[role | vlan | location | username | mac-address]**

no zeroconf server-policy *policy_name* **[role | vlan | location | username | mac-address]**

Syntax Definitions

policy_name	The name of the zero configuration server policy. The policy name can be maximum 31 characters in length.
role	The server role to be mapped with the server policy. Multiple roles can be mapped to a server policy. The role name can be maximum 32 characters in length.
vlan	The VLAN ID to be mapped with the server policy. Multiple VLAN IDs can be mapped to a server policy.
location	The location name to be mapped with the server policy. Multiple locations can be mapped to a server policy. The location name can be maximum 32 characters in length.
username	The user name to be mapped with the server policy. Multiple user names can be mapped to a server policy. The user name can be maximum 64 bytes in length.
mac-address	The MAC address to be mapped with the server policy. Multiple macaddress can be mapped to a server policy. Maximum size of macaddress allowed is six bytes.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configured server policy is not applied unless it is mapped to a service rule.
- A maximum of 16 roles, 16 locations, 16 VLANs, 16 username, and 16 MAC address can be configured for a server policy.
- The server policy can be modified even when it is mapped to a service rule.
- The server policy cannot be deleted if it is being used by a service rule.
- The server policy attribute can be deleted even when it is mapped to a service rule unless any one of the policy attributes remains configured for that policy.
- To remove the server policy, use the **no** form of the command. To remove specific attribute associated to the policy mention the attribute along with the **no** command.

Example

```
-> zeroconf server-policy SP1 role employee
-> zeroconf server-policy SP1 vlan 10 20 30
-> zeroconf server-policy SP1 location meetingroom1 meetingroom2
-> zeroconf server-policy SP1 username user1 user2
-> zeroconf server-policy SP1 mac-address e8:e7:32:9a:53:3 e8:e7:32:9a:53:3
-> no zeroconf server-policy SP1
-> no zeroconf server-policy SP1 role employee
-> no zeroconf server-policy SP1 vlan 10 20
-> no zeroconf server-policy SP1 location meetingroom1
-> no zeroconf server-policy SP1 username user2
-> no zeroconf server-policy SP1 mac-address e8:e7:32:9a:53:3
```

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **username** and **mac-address** parameters included.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
zeroconf client-policy	Configures the client policy.
zeroconf service-rule policy	Allows to define service rules for selective sharing of services with the clients.
zeroconf refresh-database	Displays the zero configuration for the switch.
show zeroconf server policies	Displays the information of the server policies configured.

MIB Objects

```
alaZeroConfServerPolicyTable
   alaZeroConfServerPolicyEntry
   alaZeroConfServerPolicyName
   alaZeroConfServerRoleMappingName
   alaZeroConfServerVlanMappingId
   alaZeroConfServerLocationMappingString
   alaZeroConfServerUsernameMappingString
   alaZeroConfServerMacAddressMapping
```

zeroconf client-policy

Configures the client policy.

zeroconf client-policy *policy_name* **[role | vlan | location | username | mac-address]**

no zeroconf client-policy *policy_name* **[role | vlan | location | username | mac-address]**

Syntax Definitions

policy_name	The name of the zero configuration client policy. The policy name can be maximum 31 characters in length.
role	The client role to be mapped with the client policy. Multiple roles can be mapped to a client policy. The role name can be maximum 32 characters in length.
vlan	The VLAN ID to be mapped with the client policy. Multiple VLAN IDs can be mapped to a client policy.
location	The location name to be mapped with the client policy. Multiple locations can be mapped to a client policy. The location name can be maximum 32 characters in length.
username	The user name to be mapped with the client policy. Multiple user names can be mapped to a client policy. The user name can be maximum 64 bytes in length.
mac-address	The MAC address to be mapped with the client policy. Multiple MAC addresses can be mapped to a client policy. Maximum size of MAC address allowed is six bytes.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configured client policy is not applied unless it is mapped to a service rule.
- A maximum of 16 roles, 16 locations, 16 VLANs, 16 username, and 16 MAC address can be configured for a client policy.
- The client policy can be modified even when it is mapped to a service rule.
- The client policy cannot be deleted if it is being used by a service rule.
- The client policy attribute can be deleted even when it is mapped to a service rule unless any one of the policy attributes remains configured for that policy.
- To remove the client policy, use the **no** form of the command. To remove specific attribute associated to the policy mention the attribute along with the **no** command.

Example

```
-> zeroconf client-policy SP1 role employee
-> zeroconf client-policy SP1 vlan 10 20 30
-> zeroconf client-policy SP1 location meetingroom1 meetingroom2
-> zeroconf client-policy SP1 username username1 username2
-> zeroconf client-policy SP1 mac-address e8:e7:32:9a:53:3 e8:e7:32:9a:53:3
-> no zeroconf client-policy SP1
-> no zeroconf client-policy SP1 role employee
-> no zeroconf client-policy SP1 vlan 10 20
-> no zeroconf client-policy SP1 location meetingroom1
-> no zeroconf client-policy SP1 username user2
-> no zeroconf client-policy SP1 mac-address e8:e7:32:9a:53:3
```

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **username** and **mac-address** parameters included.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
zeroconf server-policy	Configures the server policy.
zeroconf service-rule policy	Allows to define service rules for selective sharing of services with the clients.
zeroconf refresh-database	Displays the zero configuration for the switch.
show zeroconf client policies	Displays the information of the client policies configured on the responder.

MIB Objects

```
alaZeroConfClientPolicyTable
   alaZeroConfClientPolicyEntry
   alaZeroConfClientPolicyName
   alaZeroConfClientRoleMappingName
   alaZeroConfClientVlanMappingId
   alaZeroConfClientLocationMappingString
   alaZeroConfClientUsernameMappingString
   alaZeroConfClientMacAddressMapping
```

zeroconf service-rule policy

Defines service rules for selective sharing of services with the clients.

zeroconf service-rule *rule_name* **server-policy** *server_policy_name* **client-policy** *client_policy_name*

no zeroconf service-rule *rule_name*

Syntax Definitions

rule_name	The name of the service rule. The rule name can be maximum 31 characters in length.
server_policy_name	Name of the server policy to be mapped with service rule. A server policy cannot be mapped to multiple service rules.
client_policy_name	The name of the client policy to be mapped with the service rule. A client policy cannot be mapped to multiple service rules.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- There must be one-to-one mapping between the server and client policy.
- The responder will respond to a service query only when the server and client policy is matched.
- A service rule with an existing server and client policy mapping cannot be linked to a new server and client policy without deleting the existing mapping.
- A maximum of 64 service rule configuration is supported on a responder.
- To remove a service rule, use the **no** form of the command.

Example

```
-> zeroconf service-rule SR1 server-policy SP1 client-policy CP1
-> no zeroconf service-rule SR1
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
zeroconf server-policy	Configures the server policy.
zeroconf client-policy	Configures the client policy.
zeroconf service-rule service-id	Allows to configure selective services for a service rule to be shared with the clients.
zeroconf refresh-database	Displays the zero configuration for the switch.
show zeroconf service rules	Displays the information of the service rules configured on the responder.

MIB Objects

```
alaZeroConfServiceRuleTable
   alaZeroConfServiceRuleEntry
   alaZeroConfServiceRuleName
   alaZeroConfServiceRuleServerPolicyName
   alaZeroConfServiceRuleClientPolicyName
```

zeroconf service-rule service-id

Configures selective services for a service rule.

zeroconf service-rule *rule_name* **[mdns-service-id | ssdp-service-id]** *service_id1.....[service_idn]*

no zeroconf service-rule *rule_name* **[mdns-service-id | ssdp-service-id]** *service_id1.....[service_idn]*

Syntax Definitions

rule_name	The name of the service rule.
mdns-service-id	Configures the mDNS service ID list to be mapped with the service rule.
ssdp-service-id	Configures the SSDP service ID list to be mapped with the service rule.
service_id	The service ID to be mapped with the service rule. Multiple service IDs can be mapped with a service rule.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- A service ID can be part of multiple service rule or multiple service IDs can be mapped to a service rule.
- A service ID can be mapped or removed form a service rule without deleting the service rule.
- The responder will respond to a service query only when the server and client policy is matched.
- A maximum of 64 service IDs can be configured for a service rule.
- To remove a service ID, use the **no** form of the command.

Example

```
-> zeroconf service-rule SR1 mdns-service-id _scanner._tcp.local _ipp._tcp.local
-> zeroconf service-rule SR2 ssdp-service-id urn:schemas-upnp-
org:device:MediaServer:1 upnp:rootdevice
-> no zeroconf service-rule SR1 mdns-service-id _scanner._tcp.local
-> no zeroconf service-rule SR2 ssdp-service-id upnp:rootdevice
```

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **ssdp-service-id** parameter included.

Related Commands

zeroconf service-rule policy	Allows to define service rules for selective sharing of services with the clients.
zeroconf refresh-database	Displays the zero configuration for the switch.
show zeroconf service rules	Displays the information of the service rules configured on the responder.

MIB Objects

```
alaZeroConfServiceRuleMdnsServiceMappingTable
   alaZeroConfServiceRuleMdnsServiceMappingEntry
   alaZeroConfServiceRuleSsdpServiceMappingEntry
```

zeroconf service-list

Configures a list of known services for mDNS or SSDP service query.

zeroconf [mdns service-list | ssdp service-list] *service_id1...service_idn*

no zeroconf [mdns service-list | ssdp service-list] *service_id1...service_idn*

Syntax Definitions

mdns service-list	Configures the list of mDNS services for the service query.
ssdp service-list	Configure the list of SSDP services for the service query.
service_id	The service ID to be included in the service list. A maximum of 64 service IDs can be configured in the list.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The services in the list are queried for re-learning by the responder, in an event of reload or takeover on the responder.
- A maximum of 64 service IDs can be configured in a service list.
- To remove a service ID from the service list, use the **no** form of the command.

Example

```
-> zeroconf mdns service-list _scanner._tcp.local _ipp._tcp.local
-> zeroconf ssdp service-list urn:schemas-upnp-org:device:MediaServer:1
upnp:rootdevice
-> no zeroconf mdns service-list _scanner._tcp.local
-> no zeroconf ssdp service-list upnp:rootdevice
```

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **ssdp service-list** parameter included.

Related Commands

zeroconf service-id query-request	Allows to query a specific service.
show zeroconf services-cache	Displays the list of services assigned along with the service information.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfMdnsServiceTable
   alaZeroConfMdnsServiceEntry
   alaZeroConfSsdpServiceEntry
```

zeroconf service-id query-request

Queries a specific service. If the responder does not learn a service, that specific service can be queried for re-learning by the responder.

zeroconf {mdns | ssdp} service-id *service-id* **query-request**

Syntax Definitions

mdns	Sends mDNS query for the service ID to all the configured tunnels to re-learn the service instance.
ssdp	Sends SSDP query for the service ID to all the configured tunnels to re-learn the service instance.
service_id	The service ID to be queried for learning by the responder.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to manually query for a specific service.

Example

```
-> zeroconf mdns service-id _scanner._tcp.local query-request
-> zeroconf ssdp service-id upnp:rootdevice
```

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **ssdp** parameter included.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfMdnsServiceTriggerQuery
alaZeroConfSsdpServiceTriggerQuery
```

zeroconf edge-ip-list

Configures the list of tunnel edge endpoint IP addresses. The edge-ip-list must be configured for the responder.

zeroconf edge-ip-list *ip_address1...ip_addressn*

no zeroconf edge-ip-list *ip_address1...ip_addressn*

Syntax Definitions

ip_address	The tunnel edge endpoint IP address, which is the Loopback0 IP address of the edge switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configured tunnel edge endpoint IP address in the list must be reachable. If the IP addresses are not reachable then the operational status of the mDNS will be down.
- To remove a tunnel edge endpoint IP address from the list, use the **no** form of the command.

Example

```
-> zeroconf edge-ip-list 10.1.1.1 10.2.2.2 10.3.3.3
-> no zeroconf edge-ip-list 10.1.1.1
```

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
show zeroconf edge-details	Displays the IP address and reachability status of the tunnel endpoints configured on the responder.
zeroconf refresh-database	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfEdgeIpTable
   alaZeroConfEdgeIpEntry
```

zeroconf refresh-database

Refreshes the database (mDNS or SSDP records) with latest server policies, client policies, server rules, learned service instances, and service cache entry.

zeroconf {mdns | ssdp} refresh-database

Syntax Definitions

mdns	Refreshes the mDNS database. The files “mdns_srvr_plcy”, “mdns_srvr_plcy_inst”, “mdns_clnt_plcy” and “mdns_srvc_rule” are updated.
ssdp	Refreshes the SSDP database. The files “ssdp_srvr_plcy”, “ssdp_srvr_plcy_inst”, “ssdp_clnt_plcy” and “ssdp_srvc_rule” are updated.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to update the latest server policies, server policy name along with learned service instance, client policies and server rules configuration.
- After refreshing the database, use the **show zeroconf services-cache** and **show zeroconf server policy-instances** commands to display the latest cache and service instances information.

Example

```
-> zeroconf mdns refresh-database
-> zeroconf ssdp refresh-database
```

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **ssdp** parameter included.

Related Commands

show zeroconf services-cache	Displays the list of services learned by mDNS or SSDP stack.
show zeroconf server policy-instances	Displays the mDNS or SSDP service instance learned on the responder for each server policy.

MIB Objects

```
alaZeroConfMdnsActions
alaZeroConfSsdpActions
```

show zeroconf

Displays the basic zero configuration details.

show zeroconf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show zeroconf
zero-conf mode          : responder,
MDNS admin status       : enabled,
SSDP admin status       : disabled
MDNS operational status : up,
SSDP operational status : down,
Tunnel Source IP        : 172.16.1.1

-> show zeroconf
zero-conf mode          : gateway,
MDNS admin status       : disabled,
SSDP admin status       : disabled
MDNS operational status : down,
SSDP operational status : down,
Gateway vlans list      : 1, 2, 3

-> show zeroconf
zero-conf mode          : tunnel,
zero-conf tunnel type   : standard,
MDNS admin status       : disabled,
SSDP admin status       : disabled
MDNS operational status : down,
SSDP operational status : down,
Responder IP            : -
Tunnel source IP        : -
Access vlans list       : 4, 5, 6

-> show zeroconf
zero-conf mode          : tunnel,
zero-conf tunnel type   : aruba,
MDNS admin status       : disabled,
```

```
SSDP admin status       : disabled
MDNS operational status : down,
SSDP operational status : down,
Responder IP            : -
Tunnel source IP        : -
```

output definitions

zero-conf mode	Displays the zero configuration mode configured.
zero-conf tunnel type	Displays if the tunnel type is Aruba or Standard. This is displayed if the mode type is tunnel.
MDNS admin status	Displays the administrative status of the mDNS.
SSDP admin status	Displays the administrative status of the SSDP.
MDNS operational status	Displays the operational status of mDNS. The operation status will be down if the responder IP address is not configured or not reachable.
SSDP operational status	Displays the operational status of SSDP. The operation status will be down if the responder IP address is not configured or not reachable.
Responder IP	Displays the configured responder IP address. This is displayed if the mode type is tunnel.
Tunnel Source IP	Displays the source IP address of the tunnel. This is displayed if the mode type is tunnel or responder.
Gateway vlans list	Displays the configured gateway VLANs list. This is displayed if the mode type is gateway.
Access vlans list	Displays the configured access VLANs list. This is displayed if the mode type is tunnel and the tunnel type is standard.

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf mdns admin-state	Enables or disables mDNS tunnel relay for the switch.
zeroconf ssdp admin-state	Associates a GRE tunnel interface with the mDNS relay feature.
zeroconf mode	Configures the mode of the SSDP or MDNS packet processing.
zeroconf responder-ip	Configures the IP address of the tunnel endpoint (zero configuration responder).
zeroconf gateway-vlan-list	Adds or deletes a VLAN from the gateway VLAN list.
zeroconf access-vlan-list	Adds or deletes a VLAN from the access VLAN list.

MIB Objects

```
alaZeroConfConfig
   alaZeroConfMdnsAdminStatus
   alaZeroConfSsdpAdminStatus
   alaZeroConfMode
   alaZeroConfTunnelMode
   alaZeroConfResponderIpAddressType
   alaZeroConfResponderIpAddress
   alaZeroConfMdnsOperStatus
   alaZeroConfSsdpOperStatus
```

show zeroconf services

Displays all the configured mDNS or SSDP service IDs.

show zeroconf [mdns | ssdp] services

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show zeroconf mdns services
Service Id                              CfgType
----------------------------------------+-----------------
_ipp._tcp.local                          Configured

-> show zeroconf ssdp services
Service Id                              CfgType
----------------------------------------+-----------------
upnp:rootdevice                          Configured
```

output definitions

Service Id	Displays the name of the service ID.
CfgType	Displays if the service is a configured service or learnt service.

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **ssdp** parameter included.

Related Commands

zeroconf service-list	Allows to configure a list of know services for mDNS or SSDP service query.
zeroconf service-rule policy	Allows to define service rules for selective sharing of services with the clients.

MIB Objects

```
alaZeroConfMdnsServiceTable
   alaZeroConfMdnsServiceEntry
   alaZeroConfMdnsServiceId
   alaZeroConfMdnsServiceType
alaZeroConfSsdpServiceTable
   alaZeroConfSsdpServiceEntry
   alaZeroConfSsdpServiceId
   alaZeroConfSsdpServiceType
```

show zeroconf services-cache

Displays the list of services learned by mDNS or SSDP stack.

show zeroconf [mdns | ssdp] services-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show zeroconf mdns services-cache
Service Instance: Officejet 7500 E910 [3EA581] (2)
Service-ID      : _http-alt._tcp.local
IP address      : 18.6.1.7
Port            : 8080
Ttl             : 4500
Role            : Media_server
Location        : APPLE_printer_server_1111
User Name       : 88:51:fb:3e:a5:81
Mac             : 88:51:fb:3e:a5:81
Vlan            : 77

-> show zeroconf ssdp services-cache
Service Instance: uuid:00bc1f27-d258-4ad0-be79-d5e6ffa1aaee::upnp:rootdevice
Service-ID      : urn:schemas-upnp-org:service:ConnectionManager:1
IP address      : 25.1.1.1
Port            : 42433
Ttl             : 1800
Role            : STUDENT_ACCESS
Location        : media_client_28213798127389172371738712893 7
User Name       : 00:0f:fe:26:9e:ad
Mac             : 00:0f:fe:26:9e:ad
Vlan            : 45
```

output definitions

Service Instance	Displays the device name of the service instance.
Service-ID	Displays the type of service.
IP address	Displays the IP address of the device on which the service is discovered.

output definitions

Port	Displays the UDP port number of the discovered service instance.
TTL	Displays the age of the service cache entry in seconds.
Role	Displays the role derived from UNP policy list name on the edge switch.
Location	Displays the location derived from the edge switch.
User Name	Displays the user name assigned for the service.
Mac	Displays the MAC address assigned for the service.
Vlan	Displays the VLAN ID assigned for the service.

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **ssdp** parameter included.

Related Commands

zeroconf service-rule policy	Allows to define service rules for selective sharing of services with the clients.
zeroconf service-rule service-id	Allows to configure selective services for a service rule to be shared with the clients.

MIB Objects

N/A

show zeroconf edge-details

Displays the IP address and reachability status of the tunnel endpoints configured on the responder.

show zeroconf edge-details

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show zeroconf edge-details
EdgeIP                Status
----------------------+---------
172.16.1.2            DOWN,
172.16.1.3            DOWN,
172.16.1.4            UP,
172.16.1.5            UP,
```

output definitions

EdgeIP	The tunnel endpoint IP address configured on the responder.
Status	The reachability status of the tunnel endpoint IP address.

Release History

Release 8.4.1 R02; command introduced.

Related Commands

zeroconf edge-ip-list	Allows to configure the list of tunnel edge endpoint IP addresses.

MIB Objects

```
alaZeroConfEdgeIpTable
   alaZeroConfEdgeIpEntry
   alaZeroConfEdgeIpAddrType
   alaZeroConfEdgeIpAddr
   alaZeroConfEdgeIpRowStatus
```

show zeroconf server policies

Displays information about the server policies configured.

show zeroconf server policies

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show zeroconf server policies
Server policies:

    Policy name         : SP1
    Attached locations  : MMS_server_36_1_1_1
    Attached roles      : Media_server
    Attached vlans      : 55
    Attached username   : -
    Attached mac        : 00:0f:fe:3a:63:da

    Policy name         : printer1
    Attached locations  : -
    Attached roles      : -
    Attached vlans      : 1100
    Attached username   : -
    Attached mac        : -
```

output definitions

Policy name	Displays the name of the server policy.
Attached roles	Displays the role of the server policy.
Attached locations	Displays the location of the server policy.
Attached vlans	Displays the VLANs tagged to the server policy.
Attached username	Displays the username tagged to the server policy.
Attached mac	Displays the MAC address tagged to the server policy.

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **Attached username** and **Attached mac** output fields added.

Related Commands

zeroconf server-policy	Configures the server policy.

MIB Objects

```
alaZeroConfServerPolicyTable
   alaZeroConfServerPolicyEntry
   alaZeroConfServerPolicyName
alaZeroConfServerRoleMappingTable
   alaZeroConfServerRoleMappingEntry
   alaZeroConfServerRoleMappingName
alaZeroConfServerVlanMappingTable
   alaZeroConfServerVlanMappingEntry
   alaZeroConfServerVlanMappingId
alaZeroConfServerLocationMappingTable
   alaZeroConfServerLocationMappingEntry
   alaZeroConfServerLocationMappingString
```

show zeroconf client policies

Displays information about the client policies configured on the responder.

show zeroconf client policies

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show zeroconf client policies
Client policies:

    Policy name         : CP1
    Attached locations  : media_client_2821379812738917237173871289 37
    Attached roles      : STUDENT_ACCESS
    Attached vlans      : 45
    Attached username   : -
    Attached mac        : 00:0f:fe:3a:34:1a
```

output definitions

Policy name	Displays the name of the client policy.
Attached roles	Displays the role of the client policy.
Attached locations	Displays the location of the client policy.
Attached vlans	Displays the VLANs tagged to the client policy.
Attached username	Displays the username tagged to the client policy.
Attached mac	Displays the MAC address tagged to the client policy.

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **Attached username** and **Attached mac** output fields added.

Related Commands

zeroconf client-policy	Configures the client policy.

MIB Objects

```
alaZeroConfClientPolicyTable
   alaZeroConfClientPolicyEntry
   alaZeroConfClientPolicyName
alaZeroConfClientRoleMappingTable
   alaZeroConfClientRoleMappingEntry
   alaZeroConfClientRoleMappingName
alaZeroConfClientVlanMappingTable
   alaZeroConfClientVlanMappingEntry
   alaZeroConfClientVlanMappingId
 alaZeroConfClientLocationMappingTable
   alaZeroConfClientLocationMappingEntry
   alaZeroConfClientLocationMappingString
alaZeroConfClientUsernameMappingTable
   alaZeroConfClientUsernameMappingEntry
   alaZeroConfClientUsernameMappingString
alaZeroConfClientMacAddressMappingTable
   alaZeroConfClientMacAddressMappingEntry
   alaZeroConfClientMacAddressMappingMacAddress
```

show zeroconf service rules

Displays information about the service rules configured on the responder.

show zeroconf service rules

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show zeroconf service rules
Service rules:

    Rule name                       : SR1
    Client Policy                   : CP1
    Server Policy                   : SP1
    Attached mdns services          : _ipp._tcp.local
    Attached ssdp services          : upnp:rootdevice

    Rule name                       : SR2
    Client Policy                   : CP2
    Server Policy                   : SP2
    Attached mdns services          : _ipp._tcp.local
    Attached ssdp services          : upnp:rootdevice

    Rule name                        : SR3
    Client Policy                    : CP3
    Server Policy                    : SP3
    Attached mdns services           : _ipp._tcp.local
    Attached ssdp services           : upnp:rootdevice
                                       upnp:rootdevice
```

output definitions

Rule name	Displays the name of the service rule.
Client Policy	Displays the name of the client policy mapped to the service rule.
Server Policy	Displays the name of the server policy mapped to the service rule.
Attached mdns services	Displays the mDNS service instances learned for the service rule.
Attached ssdp services	Displays the SSDP service instances learned for the service rule.

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **Attached ssdp services** output field added.

Related Commands

zeroconf service-rule policy	Allows to define service rules for selective sharing of services with the clients.

MIB Objects

```
alaZeroConfServiceRuleTable
   alaZeroConfServiceRuleEntry
   alaZeroConfServiceRuleName
   alaZeroConfServiceRuleServerPolicyName
   alaZeroConfServiceRuleClientPolicyName
```

show zeroconf server policy-instances

Displays the mDNS or SSDP service instance learned on the responder for each server policy.

show zeroconf [mdns | ssdp] server policy-instances

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Example

```
-> show zeroconf mdns server policy-instances
MDNS server policy instances:

   Policy name                    : SP1
   Attached service instance      : -

   Policy name                    : SP2
   Attached service instance      : PRINTER_EDGE4
                                    PRINTER_EDGE3

   Policy name                    : SP3
   Attached service instance      : -

   Policy name                     : SP4
   Attached service instance       : PRINTER_EDGE4

-> show zeroconf ssdp server policy-instances
 SSDP server policy instances :

    Policy name              : SP1
    Attached service instance:

    Policy name              : SP3
    Attached service instance: uuid:88618bb0-6790-4cb0-9166-
e1d15af5a87c::upnp:rootdevice

    Policy name              : SP4
    Attached service instance: uuid:88618bb0-6790-4cb0-9166-
e1d15af5a87c::upnp:rootdevice
```

output definitions

Policy name	Displays the name of the server policy.
Attached service instance	Displays the service instance learned for the server policy.

Release History

Release 8.4.1 R03; command introduced.

Related Commands

zeroconf service-rule policy	Allows to define service rules for selective sharing of services with the clients.

MIB Objects

N/A

show unp profile

Displays the UNP profile configuration for the switch.

show unp profile [*profile_name***]**

Syntax Definitions

profile_name	The name of the UNP to display.

Defaults

By default, the configuration for all profiles is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a UNP profile name with this command to display information for a specific profile.
- Use the **show unp profile map** command to display the VLAN or service type (SPB, VXLAN, or static) that is mapped to the UNP profile.
- If Device Profiling is enabled for the switch, the following UNP profiles are automatically created on the switch and will be included in the display:
  - devProfPrinter
  - devProfWindows
  - devProfIP-Phone
  - devProfWireless-Router
  - devProfSmartPhone/PDA/Tablets

Examples

```
-> show unp profile
Profile Name: unp2-spb
    Qos Policy      = qrules1,
    Location Policy = -,
    Period Policy   = -,
    CP Profile      = -,
    CP State        = Dis,
    Authen Flag     = Dis,
    Mobile Tag      = Dis,
    SAA Profile     = -,
    Ingress BW      = -,
    Egress BW       = -,
    Ingress Depth   = -,
    Egress Depth    = -,
    Inact Interval  = 10
    Mac-Mobility    = Ena

Profile Name: unp1-vlan
```

```
    Qos Policy      = -,
    Location Policy = loclist1,
    Period Policy   = timelist1,
    CP Profile      = guest-profile,
    CP State        = Dis,
    Authen Flag     = Dis,
    Mobile Tag      = Dis,
    SAA Profile     = -,
    Ingress BW      = -,
    Egress BW       = -,
    Ingress Depth   = -,
    Egress Depth    = -,
    Inact Interval  = 10
    Mac-Mobility    = Dis

Profile Name: defaultWLANProfile
    Qos Policy      = -,
    Location Policy = -,
    Period Policy   = -,
    CP Profile      = -,
    CP State        = Dis,
    Authen Flag     = Dis,
    Mobile Tag      = Dis,
    SAA Profile     = -,
    Ingress BW      = -,
    Egress BW       = -,
    Ingress Depth   = -,
    Egress Depth    = -,
    Inact Interval  = 10
    Mac-Mobility    = Dis

Total Profile Count: 3

-> show unp profile unp1-vlan
Profile Name: unp1-vlan
    Qos Policy      = -,
    Location Policy = loclist1,
    Period Policy   = timelist1,
    CP Profile      = guest-profile,
    CP State        = Dis,
    Authen Flag     = Dis,
    Mobile Tag      = Dis,
    SAA Profile     = -,
    Ingress BW      = -,
    Egress BW       = -,
    Ingress Depth   = -,
    Egress Depth    = -,
    Inact Interval  = 10
    Mac-Mobility    = Dis
    Kerberos Auth   = Dis
```

output definitions

Profile Name	The name of the UNP profile. Configured through the **unp profile** command.
QoS Policy	The name of the QoS policy list associated with the profile. Configured through the **unp profile qos-policy-list** command.

output definitions

Location Policy	The name of the location policy assigned to the UNP profile. Configured through the **unp profile location-policy** command.
Period Policy	The name of the period policy assigned to the UNP profile. Configured through the **unp profile period-policy** command.
CP Profile	The name of the Captive Portal (CP) profile assigned to the UNP profile A CP profile defines a CP configuration that is applied to devices when CP authentication is enabled for the UNP profile. Configured through the **unp profile captive-portal-profile** command.
CP State	The CP authentication status (**Ena** or **Dis**) for the UNP profile. Indicates whether CP authentication is triggered for devices classified into the profile. Configured through the **unp profile captive-portal-authentication** command.
Authen Flag	The authentication flag status (**Ena** or **Dis**) for the UNP profile. Indicates whether only authenticated devices are allowed into the profile. Configured through the **unp profile authentication-flag** command.
Mobile Tag	The mobile tag status (**Ena** or **Dis**) for the UNP profile. When enabled, the first user that is learned on a UNP port and is classified into a UNP profile will cause the UNP port to be added as a tagged member of the VLAN associated with the profile. If the profile is mapped to a service, a tagged virtual port association is created. Configured through the **unp profile mobile-tag** command.
SAA Profile	The name of a Service Assurance Agent (SAA) profile that is associated with the UNP profile. Configured through the **unp profile saa-profile** command.
Ingress BW	The maximum ingress bandwidth setting that is applied to ports associated with the profile. Configured through the **unp profile maximum-ingress-bandwidth** command.
Egress BW	The maximum egress bandwidth setting that is applied to ports associated with the profile. Configured through the **unp profile maximum-egress-bandwidth** command.
Ingress Depth	The maximum ingress depth setting that is applied to ports associated with the profile. Configured through the **unp profile maximum-ingress-depth** command.
Egress Depth	The maximum egress depth setting that is applied to ports associated with the profile. Configured through the **unp profile maximum-egress-depth** command.
Inact Interval	The amount of time, in seconds, that a device can remain inactive after the MAC address for the device has aged out. When the timer reaches this value, inactive devices are automatically logged out of the network. Configured through the **unp profile inactivity-interval** command.

output definitions

Mac-Mobility	The status of MAC address mobility (**Ena** or **Dis**) for the UNP profile. MAC mobility functionality applies only to profiles that are mapped to SPB services and is *not supported on the OmniSwitch 6465 or OmniSwitch 6560*. Configured through the **unp profile mac-mobility** command.
Kerberos Auth	The status of Kerberos snooping (**Ena** or **Dis**) for the UNP profile. Indicates whether Kerberos snooping authentication is triggered for devices classified into the profile. Configured through the **unp profile kerberos-authentication** command.

Release History

Release 8.3.1; command was introduced.
Release 8.4.1.R02; the built-in “defaultWLANProfile” included in the display.
Release 8.4.1.R03; “Redirect State” field deprecated.
Release 8.5R2; default UNP profiles for Device Profiling included in the display.
Releae 8.6R1; “Mac-Mobility” field added.
Release 8.6R2; “Kerberos Auth” field added.

Related Commands

show unp classification	Displays the UNP classification rule configuration for the switch.
show unp global configuration	Displays the UNP global parameter values configured for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
   alaDaUNPProfileAuthenticationFlag
   alaDaUNPProfileMobileTag
   alaDaUNPProfileCPortalAuthentication
   alaDaUNPProfileRedirect
   alaDaUNPProfileQoSPolicy
   alaDaUNPProfilePeriodPolicy
   alaDaUNPProfileCPortalProfile
   alaDaUNPProfileLocationPolicy
   alaDaUNPProfileSaaProfile
   alaDaUNPProfileInactivityInterval
   alaDaUNPProfileMaxIngressBandwidth
   alaDaUNPProfileMaxEgressBandwidth
   alaDaUNPProfileMaxIngressDepth
   alaDaUNPProfileMaxEgressDepth
   alaDaUNPProfileMacMobility
   alaDaUNPProfileKerberosAuthentication
```

show unp profile map

Displays the VLAN, service, or L2 GRE tunnel mapping configuration assigned to a UNP profile.

show unp profile [*profile_name***] map {vlan | service-type {spb | vxlan | static | l2gre}}**

Syntax Definitions

profile_name	The name of the UNP to display.
vlan	Displays the VLAN mapping configuration for a UNP profile.
spb	Displays the Shortest Path Bridging (SPB) service mapping configuration for a UNP profile.
vxlan	Displays the Virtual eXtensible Local Area Network (VXLAN) service mapping configuration for a UNP profile.
static	Displays the existing SPB or VXLAN service IDs that are statically assigned to a UNP profile. This type of mapping is used to map the profile to a known service ID.
l2gre	Displays the L2 GRE tunnel mapping configuration for a UNP profile.

Defaults

By default, the VLAN, service, or L2 GRE tunnel mapping configuration for all profiles is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a UNP profile name with this command to display the mapping information for a specific profile.
- Only one VLAN or service is mapped to a profile at any given time.

Examples

```
-> show unp profile map vlan
Profile Name                    Vlan-Id
--------------------------------+--------
unp1-vlan                       300
unp2-vlan                       301
unp3-vlan                       500
unp4-vlan                       501

Total Profile Vlan-Map Count: 4

-> show unp profile unp2-vlan map vlan
Profile Name                    Vlan-Id
--------------------------------+--------
unp2-vlan                       301
```

output definitions

Profile Name	The name of the UNP profile that is mapped to the VLAN ID.
Vlan-Id	The VLAN ID associated with the profile.

```
-> show unp profile map service-type spb
Profile                          Tag         Vlan    Mcast   Igmp  Igmp    Mld   Mld
Name                   Isid      Value BVlan Xlation  Mode   Snoop Profile Snoop Profile
---------------------+--------+-----+-----+-------+-------+-----+-------+-----+-------
unp1-spb               1500      10    400   Ena     Tandem  Ena   -       Ena   -
unp2-spb               1600      20:30 401   Ena     Headend Ena   ipms-2  Dis   -
unp3-spb               1700      10    500   Dis     Headend Dis   -       Dis   -
SystemDefault10000010 10000010 10    4000  Dis     Headend Dis   -       Dis   -

Total Profile Spb-Map Count: 4
```

output definitions

Profile Name	The name of the UNP profile that is mapped to the SPB service.
Isid	The SPB service instance identifier (I-SID) that will be used to dynamically create the SPB service access point (SAP) for the profile.
Tag Value	The VLAN ID tags of the traffic that the dynamically created SPB SAP will carry for the profile.
BVlan	The SPB BVLAN ID that will be associated with the I-SID for the dynamically created SPB SAP.
Vlan Xlation	The status of egress VLAN translation (**Ena** or **Dis**) for the dynamically created SPB SAP.
Mcast Mode	The multicast mode (**Headend** or **Tandem**) for the dynamically created SPB SAP.
Igmp Snoop	The status of IGMP snooping for the dynamically created SPB SAP.
Igmp Profile	The name of the optional IPMS profile that is applied to the IGMP snooping instance for the dynamically created SPB SAP
Mld Snoop	The status of MLD snooping for the dynamically created SPB SAP.
Mld Profile	The name of the optional MLD profile that is applied to the IGMP snooping instance for the dynamically created SPB SAP

```
-> show unp profile map service-type vxlan
Profile                                Tag   Far-End-List Vlan    Mcast   Mcast
Name                          Vnid     Value              Xlation Mode    Group
-----------------------------+--------+-----+------------+-------+-------+---------
unp1-vxlan                     2300     20    vtep-ip1     Ena     Tandem  225.1.1.2
unp2-vxlan                     2301     40:50 vtep-ip2     Ena     Headend -
SystemDefault10000010          10000010 10    vtep-ip3     Dis     Headend -

Total Profile Vxlan-Map Count: 3
```

output definitions

Profile Name	The name of the UNP profile that is mapped to the VXLAN service.
Vnid	The VXLAN network identifier for the VXLAN segment that will be used to dynamically create the VXLAN service access point (SAP) for the profile.

output definitions

Tag Value	The VLAN ID tags of the traffic that the dynamically created VXLAN SAP will carry for the profile.
Far-End-List	The name of the list that contains the IP addresses for the far-end VXLAN Tunnel End Points (VTEPs). The VTEPs are used to create Service Distribution Points (SDPs) for the dynamically created VXLAN SAP.
Vlan Xlation	The status of egress VLAN translation (**Ena** or **Dis**) for the dynamically created VXLAN SAP.
Mcast Mode	The multicast mode (**Headend**, **Tandem**, or **Hybrid**) for the dynamically created VXLAN SAP.
Mcast Group	The multicast group IP address that the dynamically created VXLAN SAP will use to forward traffic to participating VTEPs.

```
-> show unp profile map service-type l2gre
Profile                      Tag      Far-End-List   Far-End-Ip Port       Vlan
Name                  Vpnid  Value                              Isolation  Xlation
----------------------+------+--------+-------------+----------+----------+-------
guest-profile         2002   20                     20.2.2.1   Ena        Dis

Total Profile L2gre-Map Count: 1
```

output definitions

Profile Name	The name of the UNP profile that is mapped to the L2 GRE tunnel.
Vpnid	The tunnel ID that identifies a GRE tunnel VPN.
Tag Value	The VLAN ID tags of the traffic that the dynamically created L2 GRE SAP will carry for the profile.
Far-End-List	The name of the list that contains the Loopback0 IP interface address for the far-end tunnel aggregation switch.
Far-End-Ip	The Loopback0 IP interface address for the far-end tunnel aggregation switch.
Port Isolation	The status of port isolation for the dynamically created L2 GRE SAP. Port isolation is implicitly enabled and is not configurable in this release.
Vlan Xlation	The status of VLAN translation (**Ena** or **Dis**) for the dynamically created L2 GRE SAP.

```
-> show unp profile map service-type static
Profile                                 Tag
Name                           SvcId    Value
-------------------------------+--------+--------
unp1-staticSPB                 10       20
unp2-staticVXLAN               20       40:50

Total Profile Static-Service-Map Count: 2
```

output definitions

Profile Name	The name of the UNP profile that is mapped to the static service.
SvvcId	The service ID for the existing SPB or VXLAN service.
Tag Value	The VLAN ID tags of the traffic that the SAP associated with the service ID will carry.

Release History

Release 8.3.1; command was introduced.
Release 8.4.1.R02; **l2gre** parameter added.
Release 8.6R1; IGMP and MLD snooping related fields added to SPB service-mapped profile display; "Port-Isolation" and "Vlan Xlation" fields added to L2 GRE service-mapped profile display.

Related Commands

unp profile map vlan	Configures the mapping of a standard VLAN to a UNP profile.
unp profile map service-type spb	Configures the mapping of SPB parameters that are used to dynamically create an SPB SAP to carry profile traffic.
unp profile map service-type vxlan	Configures the mapping of VXLAN parameters that are used to dynamically create a VXLAN SAP to carry profile traffic.
unp profile map service-type l2gre	Configures the mapping of L2 GRE tunnel parameters that are used to dynamically create an L2 GRE tunnel SAP to carry profile traffic.
unp profile map service-type static	Configures the mapping of an existing SPB or VXLAN service to the profile.
show unp profile	Displays the UNP profile configuration for the switch.
show unp vxlan far-end-ip-list	Displays the contents of a far-end IP address list that is used to map VXLAN service parameters to a profile.
show unp l2gre far-end-ip-list	Displays the contents of a far-end IP address list that is used to map L2 GRE service parameters to a profile.

MIB Objects

```
alaDaUNPProfileTable
   alaDaUNPProfileName
alaDaUNPProfileMapVlanTable
   alaDaUNPProfileMapVlanVlanID
alaDaUNPProfileMapSpbTable
   alaDaUNPProfileMapSpbEncapVal
   alaDaUNPProfileMapSpbIsid
   alaDaUNPProfileMapSpbBVlan
   alaDaUNPProfileMapSpbMulticastMode
   alaDaUNPProfileMapSpbVlanXlation
alaDaUNPProfileMapVxlanTable
   alaDaUNPProfileMapVxlanEncapVal
   alaDaUNPProfileMapVxlanVnid
   alaDaUNPProfileMapVxlanFarEndIPList
   alaDaUNPProfileMapVxlanMulticastIPAddressType
   alaDaUNPProfileMapVxlanMulticastIPAddress
   alaDaUNPProfileMapVxlanVlanXlation
   alaDaUNPProfileMapVxlanMulticastMode
alaDaUNPProfileMapL2GreTable
   alaDaUNPProfileMapL2GreEncapVal
   alaDaUNPProfileMapL2GreVpnid
   alaDaUNPProfileMapL2GreFarEndIPAddressType
   alaDaUNPProfileMapL2GreFarEndIPAddress
   alaDaUNPProfileMapL2GreFarEndIPList
   alaDaUNPProfileMapL2GrePortIsolation
   alaDaUNPProfileMapL2GreVlanXlation
alaDaUNPProfileMapStaticTable
   alaDaUNPProfileMapStaticEncapVal
   alaDaUNPProfileMapStaticServiceID
```

show unp vxlan far-end-ip-list

Displays the contents of an IP address list. Each address represents a VXLAN Tunnel End Point (VTEP). A far-end IP list is associated with a VXLAN service to identify all the VTEPs that will participate in that service.

show unp vxlan far-end-ip-list [*ip_list_name***]**

Syntax Definitions

ip_list_name	The name of a list that contains the IP addresses for the far-end VTEPs.

Defaults

By default, the contents of all the VXLAN far-end IP address lists is displayed.

Platforms Supported

OmniSwitch 6900-Q32, 6900-X72, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

Enter a list name with this command to display information for a specific list.

Examples

```
-> show unp vxlan far-end-ip-list
Far-End-Ip-List Name: toDataCenter1, IP-Count: 3,
    IP-Addresses:
         101.1.1.1
         102.1.1.1
         103.1.1.1
Far-End-Ip-List Name: toDataCenter2, IP-Count: 3,
    IP-Addresses:
         201.1.1.1
         202.1.1.1
         203.1.1.1

-> show unp vxlan far-end-ip-list toDataCenter2
Far-End-Ip-List Name: toDataCenter2, IP-Count: 3,
    IP-Addresses:
         201.1.1.1
         202.1.1.1
         203.1.1.1
```

output definitions

Far-End-Ip-List Name	The name of the far-end IP address list.
IP-Count	The number of IP addresses in the list.
IP-Addresses	The IP addresses that are members of the specified list name.

Release History

Release 7.3.4; command was introduced.

Related Commands

unp vxlan far-end-ip-list	Configures a UNP VXLAN far-end IP list.
show unp profile map	Displays the VXLAN service profile mapping configuration for the switch.

MIB Objects

```
alaDaUNPVxlanFarEndIPListTable
   alaDaUNPVxlanFarEndIPListName
   alaDaUNPVxlanFarEndIPListIPAddressCount
```

show unp l2gre far-end-ip-list

Displays the contents of an IP address list that contains the IP address of the Loopback0 interface configured on the far-end tunnel aggregation switch.

show unp l2gre far-end-ip-list [*ip_list_name***]**

Syntax Definitions

ip_list_name	The name of a list that contains the IP address for the far-end tunnel aggregation switch.

Defaults

By default, the contents of all the far-end IP address lists is displayed.

Platforms Supported

OmniSwitch 6560, 6860, 6865, 9900, OmniSwitch 6900-Q32, 6900-X72

Usage Guidelines

Enter a list name with this command to display information for a specific list.

Examples

```
-> show unp l2gre far-end-ip-list
Far-End-Ip-List Name: toDataCenter1, IP-Count: 1,
    IP-Addresses:
         100.1.1.1
Far-End-Ip-List Name: toDataCenter2, IP-Count: 1,
    IP-Addresses:
         202.1.1.1

-> show unp l2gre far-end-ip-list toDataCenter2
Far-End-Ip-List Name: toDataCenter2, IP-Count: 1,
    IP-Addresses:
         202.1.1.1
```

output definitions

Far-End-Ip-List Name	The name of the far-end IP address list.
IP-Count	The number of IP addresses in the list.
IP-Addresses	The IP address that is a member of the specified list name.

Release History

Release 8.5R2; command was introduced.

Related Commands

unp l2gre far-end-ip-list	Configures an L2 GRE far-end IP list.
show unp profile map	Displays the L2 GRE service profile mapping configuration for the switch.

MIB Objects

```
alaDaUNPL2GreFarEndIPListTable
   alaDaUNPL2GreFarEndIPListName
   alaDaUNPL2GreFarEndIPListIPAddressCount
```

show unp saa-profile

Displays the Service Assurance Agent (SAA) performance monitoring profile configuration for the switch. SAA profiles are assigned to UNP VLAN profiles to specify jitter and latency threshold values for SAA sessions that apply to the assigned UNP VLAN profile.

show unp saa-profile [*profile_name***]**

Syntax Definitions

profile_name	The name of an existing SAA profile to display.

Defaults

By default, all SAA profiles are displayed.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Enter an SAA profile name with this command to display information for a specific profile.
- This command does not provide the UNP assignment for each SAA profile. Use the **show unp profile** command to display the assignment information.

Examples

```
-> show unp saa-profile
Profile                          Latency     Jitter       MC Conf
Name                             Threshold   Threshold    Status
---------------------------------+-----------+------------+----------
unp_saa1                               500          100   Local
unp_saa2                                 0          150   Local
unp_saa3                               250            0   Local
```

output definitions

Profile Name	The name of the SAA profile.
Latency Threshold	The latency threshold value applied with this profile. A value of “0” indicates no threshold value is applied.
Jitter Threshold	The jitter threshold value applied with this profile. A value of “0” indicates no threshold value is applied.
MC Conf Status	The MCLAG consistency check status of the UNP configuration (**Sync, Out-Of-Sync**, or **Local**). *Note that MCLAG is not supported in this release.*

Release History

Release 7.3.2; command was introduced.

Related Commands

unp saa-profile	Configures SAA performance monitoring profiles.
show unp profile	Displays the UNP profile configuration for the switch.

MIB Objects

```
alaDaSaaProfileTable
   alaDaSaaProfileName
   alaDaSaaProfileLatencyThreshold
   alaDaSaaProfileJitterThreshold
   alaDaSaaProfileRowStatus
```

show unp global configuration

Displays the switch configuration for the global Universal Network Profile (UNP) parameter settings.

show unp global configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- UNP global parameter settings determine specific actions related to the following:
  - Dynamically creating VLANs and/or profiles.
  - Whether or not devices attempting to authenticate are assigned to a temporary profile if the authentication server is unreachable.
  - Interaction with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch Bring Your Own Devices (BYOD) solution.
- A hyphen, "-", indicates that a value has not been configured for the global UNP parameter.

Examples

```
-> show unp global configuration
  Dynamic Vlan Configuration       = Disabled,
  Dynamic Profile Configuration    = Disabled,
  Auth Server Down Profile1        = -,
  Auth Server Down Profile2        = -,
  Auth Server Down Profile3        = -,
  Auth Server Down Voice Profile1  = -,
  Auth Server Down Voice Profile2  = -,
  Auth Server Down Voice Profile3  = -,
  Auth Server Down Port Bounce     = Disabled
  Auth Server Down Timeout         = 60,
  Redirect Port Bounce             = Enabled,
  Redirect Pause Timer             = -
  Redirect http proxy-port         = 8080
  Redirect Server FQDN             = cppm.abc.com
  Redirect Server IP               = 10.135.20.50
  Allowed IP                       = -
  Force L3-Learning                = Disabled
  Force L3-Learning Port Bounce    = Enabled
  802.1x Pass Through Mode         = Disabled
  AP Mode                          = Enabled
  System-default service-mod       = 512
  System-default service-base      = 10000000
```

```
 System-default Multicast-Mode    = Headend
 System-default Vlan-Xlation      = Enabled
 System-default Multicast-Group   = 239.0.0.0
 System-default far-end-ip-list   = -
IPv6 Drop Packets                 = Disabled,
Delayed Learning Interval         = 0,
Global Mac-Mobility              = Disabled,
```

output definitions

Dynamic Vlan Configuration	The status (**Enabled** or **Disabled**) of dynamic VLAN configuration. Configured through the **unp dynamic-vlan-configuration** command.
Dynamic Profile Configuration	The status (**Enabled** or **Disabled**) of dynamic profile configuration. Configured through the **unp dynamic-profile-configuration** command.
Auth Server Down Profile1 **Auth Server Down Profile2** **Auth Server Down Profile3**	The name of a UNP that a device is assigned to in the event the RADIUS server is unreachable. Up to three different profile names are configurable as authentication server down UNP profiles. Configured through the **unp auth-server-down** command.
Auth Server Down Voice Profile1 **Auth Server Down Voice Profile2** **Auth Server Down Voice Profile3**	*Not supported in this release.*
Auth Server Down Port Bounce	*Not supported in this release.*
Auth Server Down Timeout	The amount of time, in seconds, that devices remain assigned to the authentication server down UNP. Configured through the **unp auth-server-down-timeout** command.
Redirect Port Bounce	The status (**Enabled** or **Disabled**) of the port bounce operation for non-supplicant devices. Configured through the **unp redirect port-bounce** command.
Redirect Pause Timer	The amount of time, in seconds, the switch pauses to clear all device authentication states and trigger re-authentication. Configured through the **unp redirect pause-timer** command.
Redirect http proxy-port	The HTTP proxy port number to use for redirection to a server. Configured through the **unp redirect proxy-server-port** command.
Redirect Server FQDN	The Fully Qualified Domain Name of a redirection server. Configured through the **unp redirect-server** command. This field is blank if an IP address was configured for the redirect server.
Redirect Server IP	The IP network address of a redirection server. Configured through the **unp redirect-server** command. If an FQDN was configured for the redirect server, then the resolved IP address for that domain will appear in this field.
Allowed IP	A list of IP addresses to which a host can access additional servers. Configured through the **unp redirect allowed-name** command.
Force L3-Learning	The status (**Enabled** or **Disabled**) of UNP Layer 3 learning. Configured through the **unp force-l3-learning** command.
Force L3-Learning Port Bounce	The status (**Enabled** or **Disabled**) of the port bounce action, which is associated with the Layer 3 learning function. Configured through the **unp force-l3-learning** command.

output definitions

802.1x Pass Through Mode	Whether a supplicant device is authenticated locally (**Enabled**) or passed through to another switch for authentication (**Disabled**). Configured through the **unp 802.1x-pass-through** command.
AP Mode	The status (**Enabled** or **Disabled**) of the Access Point (AP) mode. This mode is enabled to support the detection of connected OmniAccess Stellar AP devices. Configured through the **unp ap-mode** command.
System-default service-mod	The modulo number that is used to dynamically calculate an SPB I-SID value or a VXLAN VNID value for a System Default profile. Configured through the **unp system-default service-mod** command.
System-default service-base	The base service number that is used to dynamically calculate an SPB I-SID value or a VXLAN VNID value for a System Default profile. Configured through the **unp system-default service-base** command.
System-default Multicast-Mode	The multicast replication mode (**Headend** or **Tandem**) for dynamic services that are created for System Default profiles. Configured through the **unp system-default multicastmode** command.
System-default Vlan-Xlation	The status (**Enabled** or **Disabled**) of VLAN translation for dynamic services that are created for System Default profiles. Configured through the **unp system-default vlan-xlation** command.
System-default Multicast-Group	The multicast group IP address for dynamic VXLAN services that are created for System Default profiles. Configured through the **unp system-default multicastgroup** command.
System-default far-end-ip-list	The name of a far-end IP list associated with dynamic VXLAN services that are created for System Default profiles.. Configured through the **unp system-default far-end-ip-list** command.
IPv6 Drop Packets	The status (**Enabled** or **Disabled**) of IPv6 packet drop on UNP ports. Configured through the **unp ipv6-drop** command.
Delayed Learning Interval	The amount of time, in seconds, that UNP will wait before starting to learn packets received on UNP ports. Configured through the **unp delay-learning** command.
Global Mac-Mobility	The status (**Enabled** or **Disabled**) of MAC address mobility. The global status specifies the default status that is applied to new UNP profiles that are mapped to SPB service parameters. MAC mobility functionality is *not supported on the OmniSwitch 6465 or OmniSwitch 6560*. Configured through the **unp mac-mobility** command.

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R02; **Dynamic Profile Configuration** and **MC Conf Status** fields added.
Release 7.3.4; VXLAN fields added; **MC Conf Status** fields deprecated.
Release 8.3.1; **Auth Server Down UNP** field replaced with **Auth Server Down UNP Profile1**, **Auth Server Down UNP Profile2**, and **Auth Server Down UNP Profile3** fields; **Force L3-Learning** field added.
Release 8.3.1.R02; **Force L3-Learning Port Bounce** field added.

Release 8.4.1.R02; **802.1x Pass Through Mode** and **AP Mode** fields added.
Release 8.5R1; **Redirect Server FQDN** and all of the **System-default** fields added.
Release 8.5R2; **IPv6 Drop Packets** and **Delayed Learning Interval** fields added.
Release 8.6R1; **Global Mac-Mobility** field added.

Related Commands

show unp profile	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPGlobalConfiguration
   alaDaUNPDynamicVlanConfigFlag
   alaDaUNPDynamicProfileConfigFlag
   alaDaUNPAuthServerDownProfile1
   alaDaUNPAuthServerDownProfile2
   alaDaUNPAuthServerDownProfile3
   alaDaUNPAuthServerDownTimeout
   alaDaUNPRedirectPortBounce
   alaDaUNPRedirectPauseTimer
   alaDaUNPRedirectProxyServerPort
   alaDaUNPRedirectServerIPType
   alaDaUNPRedirectServerIP
   alaDaUNPForceL3Learning
   alaDaUNP8021XPassThrough
   alaDaUNPApMode
   alaDaUNPServiceModule
   alaDaUNPServiceBase
   alaDaUNPServiceMulticastMode
   alaDaUNPServiceVlanXlation
   alaDaUNPServiceMulticastGroup
   alaDaUNPServiceFarEndIpList
   alaDaUNPIpv6Drop
   alaDaUNPDelayLearning
   alaDaUNPMacMobility
alaDaUNPRedirectAllowedServerTable
   alaDaUNPRedirectAllowedServerIPType
   alaDaUNPRedirectAllowedServerIP
   alaDaUNPRedirectAllowedMaskIPType
   alaDaUNPRedirectAllowedMaskIP
```

show unp domain

Displays the UNP domain configuration for the switch.

show unp domain

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Domains are used to group physical UNP ports or link aggregates into one logical domain.
- Once a port is assigned to a specific domain, classification rules associated with the same domain ID are applied only to UNP ports associated with that same domain ID.

Examples

```
-> show unp domain

Domain   Description
--------+-----------------------------------
0        Default-Domain
1        UNP Domain 1
2        UNP Domain 2
```

Release History

Release 8.3.1; command was introduced.

Related Commands

unp domain description	Configures a domain ID to which UNP ports and classification rules are assigned.
unp domain	Assigns a UNP port to a customer domain ID.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUnpCustomerDomainTable
   alaDaUnpCustomerDomainId
   alaDaUnpCustomerDomainDesc
```

show unp classification

Displays the UNP classification rule configuration for the switch.

show unp classification *rule_type*

Syntax Definitions

rule_type	The rule type to display (refer to the table in the "Usage Guidelines" section of this command page for a list of rule type parameters).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Specifying one of the following classification rule type parameters is required with this command:

Standard Rule Parameters	Binding Rule Parameters
mac-rule	**mac-port-rule**
mac-domain-rule	**mac-ip-port-rule**
mac-oui-rule	**mac-ip-domain-rule**
mac-range-rule	**ip-port-rule**
mac-range-domain-rule	
ip-rule	
ip-domain-rule	
vlan-tag-rule	
vlan-domain-rule	
port-rule	
domain	
authentication-type-rule	
lldp-rule	

- Standard classification rule parameters are combined at the time a rule is created to define a binding classification rule. The parameter combinations provided with this command reflect the allowed binding rule parameter combinations.
- An extended classification rule defines a list of rules and allows more combinations of standard rules than the binding rule configuration (see the **show unp classification-rule** command).

Examples

```
-> show unp classification mac-rule
MAC Address        VLAN Tag Profile1 Name      Profile2 Name      Profile3 Name
-----------------+--------+-----------------+------------------+----------------
00:2a:da:11:22:01  -        unp1-vlan          unp2-vxlan         unp3-vlan
00:0f:b5:46:d7:56   20      unp4-spb           -                   -
00:2a:95:57:e1:67  -        unp2-vxlan         -                   -

Total Mac Rule Count: 3

-> show unp classification mac-range-rule

Low MAC Address    High MAC Address   VLAN Tag Profile1 Name Profile2 Name Profile3 Name
-----------------+-----------------+--------+-------------+-------------+------------
00:11:22:33:44:66  00:11:22:33:44:77  -        VNI-2400      -             -
00:11:22:33:44:88  00:11:22:33:44:99  10       CustB         VNP-B         -

Total Mac Range Rule Count: 2

-> show unp classification ip-rule
IP           IP               Profile1      Profile2      Profile3      VLAN
Address      Mask             Name          Name          Name          Tag
-------------+---------------+-------------+-------------+-------------+------
10.0.0.1      255.255.255.0   unp1-vlan     -             -             -
20.0.0.1      255.255.255.0   CustA         VNI-2300      unp1-vlan     -
30.0.0.1      255.255.255.0   SLA-1         SLA-1525                    50

Total IP Rule Count: 3

-> show unp classification mac-domain-rule
                           Profile1      Profile2      Profile3      Vlan
Domain   MAC Address       Name          Name          Name          Tag
--------+-----------------+-------------+-------------+-------------+-----
1        00:22:da:00:9a:10 unp2-vxlan    -             -             -
1        00:2a:da:11:22:01 unp1-vlan     -             -             -

-> show unp classification mac-ip-port-rule
MAC Address       IP Address  Mask        Port VLAN Tag Profile1   Profile2   Profile3
-----------------+-----------+-----------+----+--------+----------+----------+----------
00:2a:da:11:22:03 10.4.4.1    255.255.0.0 0/10  -       unp2-vxlan  -          -

Total Mac-IP-Port Binding Rule Count: 1

-> show unp classification vlan-tag-rule
VLAN Tag    Profile1 Name                Profile2 Name           Profile3 Name
-----------+----------------------------+-----------------------+-----------------------
200         unp3-vlan                    -                       -
10:20       unp1-vlan                    -                       -

-> show unp classification lldp-rule
MED Endpoint Profile1 Name                Profile2 Name           Profile3 Name
------------+----------------------------+-----------------------+-----------------------
IP-Phone     unp1-vlan                    -                           -
Acess-Point  defaultWLANProfile           -                           -

Total LLDP Rule Count: 2
```

output definitions

Domain	The customer domain ID assigned to the classification rule for the specified profiles. The rule is applied to traffic received on UNP ports that are assigned to the same domain ID. This rule is also supported in combination with each of the other classification rules. Configured through the **unp domain** command or as a parameter with the other classification rule commands**.**
MAC Address	The MAC address value to match for this profile rule. Configured through the **unp classification mac-address** command.
Low MAC Address **High MAC Address**	The lowest and highest MAC address values used to specify a range of addresses to match for this rule. Configured through the **unp classification mac-range** command.
IP Address **IP Mask**	The IP network address and mask values to match for this rule. Configured through the **unp classification ip-address** command.
Profile1, Profile2, Profile3	The name of the UNP profile to which the rule is applied. Configured through the **unp profile** command.
VLAN Tag	The VLAN ID value to match for this profile rule. • If one VLAN ID is displayed, the rule will match single-tagged packets or the outer VLAN tag of double-tagged packets. • If two VLAN IDs are displayed, the rule will match double-tagged packets (for example, 10:20 will match outer VLAN tag 10 *and* inner VLAN tag 20). This rule is also supported in combination with each of the other classification rules. Configured through the **unp classification vlan-tag** or as a parameter with the other classification rule commands.
MED Endpoint	The LLDP Media Endpoint Device to match for this profile rule (**IP-Phone** or **Access-Point**). Configured through the **unp classification lldp med-endpoint** command.

Release History

Release 8.3.1; command was introduced.

Related Commands

show unp classification-rule	Displays the extended classification rule configuration for the switch.
show zeroconf server policy-instances	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

N/A

show unp classification-rule

Displays the UNP extended classification rule configuration for the switch. An extended classification rule defines a list of rule conditions, all of which a device must match to be classified into the UNP profile associated with the extended rule name. A name and precedence value is also assigned to the list of rule conditions.

show unp classification-rule [*rule-name***]**

Syntax Definitions

rule_name	The name of an existing extended classification rule.

Defaults

By default, the configuration for all extended rules is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter the name of an extended classification rule to display information for a specific rule.
- An extended classification rule defines a list of rules and allows more combinations of standard rules than a binding rule configuration.
- An extended classification rule is associated with a UNP profile and applied to traffic learned on UNP ports.
- If Device Profiling is enabled for the switch, the following “built-in” extended classification rules are also displayed:
  - devProfPrinter
  - devProfWindows
  - devProfIP-Phone
  - devProfWireless-Router
  - devProfSmartPhone/PDA/Tablets

Examples

```
-> show unp classification-rule

Rule Name: "ext_rule1"
  Precedence              = 10,
  Profile1                = unp1-vlan,
    Conditions:
      Domain              = 2,
      Mac-OUI             = 00:22:11,
      VLAN Tag            = 100

Rule Name: "ext_rule2"
  Precedence              = 1,
```

```
  Profile1                = unp1-vlan,
  Profile2                = unp2-vxlan,
  Profile3                = unp3-vlan,
    Conditions:
      Domain              = 20,
      Mac-Address         = 00:2a:94:11:22:01,
      Port                = 1/11 ,
      LLDP MED Endpoint   = IP-Phone,
      Authentication-Type = None,

Rule Name: "devProfPrinter"
  Precedence              = 255,
  Profile1                = devProfPrinter,
    Conditions:
      Device-Type         = Printer,

Rule Name: "devProfWindows"
  Precedence              = 255,
  Profile1                = devProfWindows,
    Conditions:
      Device-Type         = Windows,

Rule Name: "devProfIP-Phone"
  Precedence              = 255,
  Profile1                = devProfIP-Phone,
    Conditions:
      Device-Type         = IP-Phone,

Rule Name: "devProfWireless-Router"
  Precedence              = 255,
  Profile1                = devProfWireless-Router,
    Conditions:
      Device-Type         = Wireless-Router,

Rule Name: "devProfSmartPhone/PDA/Tablets"
  Precedence              = 255,
  Profile1                = devProfSmartPhone/PDA/Tablets,
    Conditions:
      Device-Type         = SmartPhone/PDA/Tablets,

Total Extended Classification Rule Count: 7

-> show unp classification-rule ext_rule2
Rule Name: "ext_rule2"
  Precedence              = 1,
  Profile1                = unp1-vlan,
  Profile2                = unp2-vxlan,
  Profile3                = unp3-vlan,
    Conditions:
      Domain              = 1,
      Mac-Address         = 00:2a:94:11:22:01,
      Port                = 1/11 ,
      LLDP MED Endpoint   = IP-Phone,
      Authentication-Type = None,

-> show unp classification-rule devProfPrinter

Rule Name: "devProfPrinter"
  Precedence              = 255,
```

```
Profile1                = devProfPrinter,
  Conditions:
    Device-Type         = Printer,
```

Release History

Release 8.1.1; command was introduced.
Release 8.2.1; **VLAN Tag** field added.
Release 8.3.1; **Edge-Profile** field replaced with **Profile1**, **Profile2**, and **Profile3** fields.
Release 8.5R2; support added for displaying Device Profile extended classification rules.

Related Commands

unp classification-rule	Configures an extended classification rule.
show unp classification	Displays the standard classification rule configuration for the switch.
show unp profile	Displays the UNP profile configuration for the switch.

MIB Objects

```
alaDaUNPClassifRuleTable
   alaDaUNPClassifRuleName
   alaDaUNPClassifRulePrecedenceNum
   alaDaUNPClassifRuleProfile1
   alaDaUNPClassifRuleProfile2
   alaDaUNPClassifRuleProfile3
   alaDaUNPClassifRulePort
   alaDaUNPClassifRulePortHigh
   alaDaUNPClassifRuleCustomerDomain
   alaDaUNPClassifRuleMacAddr
   alaDaUNPClassifRuleMacRngLoaddr
   alaDaUNPClassifRuleMacRngHiaddr
   alaDaUNPClassifRuleMacOuiAddr
   alaDaUNPClassifRuleEndPoin
   alaDaUNPClassifRuleAuthType
   alaDaUNPClassifRuleIpAddressType
   alaDaUNPClassifRuleIpAddress
   alaDaUNPClassifRuleIpMaskType
   alaDaUNPClassifRuleIpMask
   alaDaUNPClassifRuleVlanTag
   alaDaUNPClassifRuleDeviceType
```

show unp user-role

Displays the user-defined role configuration for the switch.

show unp user-role [*role_name***]**

Syntax Definitions

role_name	The name of an existing user-defined role.

Defaults

By default, all user-defined role are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enter a user-defined role name with this command to display information for a specific role.

Examples

```
-> show unp user-role
Role Name: ur1
  Qos Policy List       : qlist1
  Priority              : 1
  Conditions:
    Profile1            : unp1-vlan
    Profile2            : unp2-spb
    Profile3            : -
    Authentication-Type : Mac
    CP Status           : Enabled

Role Name: ur2
  Qos Policy List       : qlist-allow
  Priority              : 1
  Conditions:
    Profile1            : -
    Profile2            : -
    Profile3            : -
    Authentication-Type : 802.1x Fail
    CP Status           : Disabled

Total User Role Derivation Rule Count: 2

-> show unp user-role ur2
Role Name                       QoS Policy List Name             Priority
--------------------------------+--------------------------------+--------
ur2                             qlist-allow                      1
```

output definitions

Role Name	The name of the user-defined role. Configured through the **unp user-role** command.
Qos Policy List	The name of the QoS policy list associated with the role name. The specified list defines the user role for the device. Configured through the **unp user-role policy-list** command.
Priority	The role precedence, which assigns a priority value to the user-defined role. This value determines which role to apply if a device matches the conditions of more than one user-defined role. Configured through the **unp user-role** command.
Profile1, Profile2, Profile3	The name of a UNP profile. The user-defined role is only applied to devices classified into the specified profile name. Configured through the **unp user-role profile** command.
Authentication-Type	The type of authentication applied to a device (**none**, **mac**, or **802.1x**). The user-defined role is only applied to devices authenticated with the specified type. Configured through the **unp user-role authentication-type** command.
CP Status	The Captive Portal post login status. If enabled, the role is only applied to devices in this state. Configured through the **unp user-role cp-status-post-login** command.

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; **Edge-Profile** field replaced with **Profile1**, **Profile2**, and **Profile3** fields.

Related Commands

unp user-role	Configures a user-defined role.
show unp user	Displays information about devices learned on UNP ports.

MIB Objects

```
alaDaUNPUserRoleTable
   alaDaUNPUserRoleName
   alaDaUNPUserRolePrecedenceNum
   alaDaUNPUserRolePolicyList
   alaDaUNPUserRoleProfile1
   alaDaUNPUserRoleProfile2
   alaDaUNPUserRoleProfile3
   alaDaUNPUserRoleAuthType
   alaDaUNPUserRolePostLoginStatus
```

show unp restricted-role

Displays the names of the explicit QoS policy lists assigned to the built-in restricted role states (Captive Portal pre-login, Unauthorized, and QMR) used by the switch.

show unp restricted-role

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

An explicit QoS policy list overrides the built-in policy list associated with the restricted role state. When the explicit policy list assignment is removed, the switch reverts back to using the built-in policy list associated with the restricted role state.

Examples

```
-> show unp restricted-role
Role name    Qos Policy List Name
------------+------------------------
UNAUTHORIZED qlist-bad
QMR          qlist-qmr
CP PRE-LOGIN qlist-cp

Total Restricted Role Count: 3
```

output definitions

Role Name	The restricted role name.
Qos Policy List	The name of the QoS policy list associated with the restricted role name.

Release History

Release 8.1.1; command was introduced.

Related Commands

unp restricted-role policy-list	Configures a user-defined role.
show unp user	Displays information about devices learned on UNP ports.

MIB Objects

```
alaDaUNPRstrctedRoleTable
   alaDaUNPRstrctedRoleType
   alaDaUNPRstrctedRolePolicyList
```

show unp port

Displays the UNP configuration for the port. Includes only ports and link aggregates on which UNP is enabled.

show unp {port [*chassis/slot/port1***[-***port2***]] | linkagg [***agg_id***[-***agg_id2***]]} [type {bridge | access}]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (10-15).
bridge	Displays only UNP bridge ports.
access	Displays only UNP access ports.

Defaults

By default, configuration information for all UNP ports or link aggregates is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a port or link aggregate ID number to display information specific to the port or link aggregate.
- Specify a UNP port type (**bridge** or **access**) to display information only for that type of UNP port.

Examples

```
-> show unp port
Port  Port    Type   802.1x  Mac      Class.   Default    802.1X     MAC       Trust-Tag
      Domain         Auth    Auth                        Pass-Alt   Pass-Alt
-----+------+------+--------+--------+--------+----------+----------+---------+---------
1/16       1 Bridge Disabled Disabled Enabled  unp-1001   -          -         Disabled
1/17       0 Bridge Disabled Disabled Disabled unp-1001   -          -         Disabled
1/18       0 Access Disabled Enabled  Enabled  spb1001    -          -         Enabled
1/35       0 Access Disabled Enabled  Disabled -          -          -         Disabled
1/36       5 Bridge Enabled  Enabled  Disabled DefUnp     1XProf1    MacPAS    Enabled
1/37       5 Access Enabled  Disabled Enabled  -          1XProf2    -         Enabled

-> show unp port 1/17
Port  Port    Type   802.1x  Mac      Class.   Default    802.1X     MAC       Trust-Tag
      Domain         Auth    Auth                        Pass-Alt   Pass-Alt
-----+------+------+--------+--------+--------+----------+----------+---------+---------
1/17       0 Bridge Disabled Disabled Disabled unp-1001   -          -         Disabled
```

```
-> show unp linkagg type bridge
LagID Port    Type   802.1x  Mac      Class.   Default    802.1X     MAC       Trust-Tag
      Domain         Auth    Auth                         Pass-Alt   Pass-Alt
-----+------+------+--------+--------+--------+----------+----------+---------+---------
10         1 Bridge Disabled Disabled Enabled  unp-1001     -          -       Disabled
15         0 Bridge Disabled Disabled Disabled unp-1001     -          -       Disabled
```

output definitions

Port/LagID	The port or link aggregate on which UNP is enabled. Configured through the **unp port-type** command.
Port Domain	The customer domain ID assigned to the UNP port. Traffic received on the port is classified with UNP profile rules that are assigned to the same domain ID. Configured through the **unp domain** command**.**
Type	The type of UNP port (**Bridge** or **Access**). UNP bridge ports classify traffic into VLAN profiles; UNP access ports classify traffic into service profiles. Configured through the **unp port-type** command.
802.1x Auth	The status of 802.1X authentication (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp 802.1x-authentication** command.
Mac Auth	The status of MAC authentication (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp mac-authentication** command.
Class.	The status of classification (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp classification** command.
Default	The name of the default UNP assigned to the port or link aggregate. Configured through the **unp default-profile** command.
802.1X Pass-Alt	The name of the 802.1X authentication pass alternate UNP assigned to the port or link aggregate. Configured through the **unp 802.1x-authentication pass-alternate** command.
MAC Pass-Alt	The name of the MAC authentication pass alternate UNP assigned to the port or link aggregate. Configured through the **unp mac-authentication pass-alternate** command.
Trust-Tag	The status of the trust VLAN tag option for the UNP port or link aggregate. Configured through the **unp trust-tag** command.

Release History

Release 8.3.1; command was introduced.

Related Commands

show unp profile	Displays the UNP configuration for the switch.
show unp port config	Displays detailed configuration information for UNP ports and link aggregates.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDomainID
   alaDaUNPPortType
   alaDaUNPPort8021XAuthStatus
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortTrustTagStatus
```

show unp port config

Displays detailed configuration information for UNP ports and link aggregates.

show unp {port [*chassis/slot/port1***[-***port2***]] | linkagg [***agg_id***[-***agg_id2***]]} config**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID. Use a hyphen to specify a range of link aggregates IDs (10-15).

Defaults

By default, configuration information for all ports or link aggregates is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **port** or **linkagg** parameter to display information for a specific port or link aggregate ID.

Examples

```
-> show unp port 1/1/10 config
Port  1/1/10
  Port-Type                     = BRIDGE,
  Redirect Port Bounce          = Disabled,
  802.1x authentication         = Enabled,
  802.1x Pass Alternate Profile  = -,
  802.1x Bypass                 = Disabled,
  802.1x failure-policy         = default,
  Mac-auth allow-eap            = -,
  Mac authentication            = Enabled,
  Mac Pass Alternate Profile    = -,
  Classification                = Enabled,
  Trust-tag                     = Enabled,
  Default Profile               = -,
  Port Domain Num               = 0,
  AAA Profile                   = -,
  Port Template                 = bridgeDefaultPortTemplate,
  Port Control Direction        = Both,
  Egress Flooding               = Not Allowed,
  Admin State                   = Enabled,
  Dynamic Service               = -,
  PVLAN Port Type               = -,
  Force L3-Learning             = Disabled,
  Force L3-Learning Port Bounce  = Enabled,
  AP Mode                       = Enabled,
  802.1x Parameters:
```

```
          Tx-Period         = 30,
          Supp-Timeout      = 30,
          Max-req           = 2
  L2 Profile                    = -,

-> show unp port 1/1/11 config
Port  1/1/11
  Port-Type                     = Access,
  802.1x authentication         = Enabled,
  802.1x Pass Alternate Profile  = -,
  802.1x Bypass                 = Disabled,
  802.1x failure-policy         = default,
  Mac-auth allow-eap            = -,
  Mac authentication            = Enabled,
  Mac Pass Alternate Profile    = -,
  Classification                = Enabled,
  Trust-tag                     = Enabled,
  Default Profile               = -,
  Port Domain Num               = 0,
  AAA Profile                   = -,
  Port Template                 = accessDefaultPortTemplate,
  Admin State                   = Enabled,
  Dynamic Service               = spb,
  PVLAN Port Type               = -,
  Force L3-Learning             = Disabled,
  Force L3-Learning Port Bounce  = Enabled,
  AP Mode                       = -,
  802.1x Parameters:
          Tx-Period         = 30,
          Supp-Timeout      = 30,
          Max-req           = 2
  L2 Profile                = "unp-def-access-profile",

-> show unp linkagg 12 config
Linkagg ID  0/12
  Port-Type                     = Bridge,
  Redirect Port Bounce          = Disabled,
  802.1x authentication         = Enabled,
  802.1x Pass Alternate Profile  = -,
  802.1x Bypass                 = Disabled,
  802.1x failure-policy         = default,
  Mac-auth allow-eap            = -,
  Mac authentication            = Enabled,
  Mac Pass Alternate Profile    = -,
  Classification                = Enabled,
  Trust-tag                     = Enabled,
  Default Profile               = -,
  Port Domain Num               = 0,
  AAA Profile                   = -,
  Port Template                 = bridgeDefaultPortTemplate,
  Port Control Direction        = Both,
  Egress Flooding               = Not Allowed,
  Admin State                   = Enabled,
  Dynamic Service               = -,
  Force L3-Learning             = Disabled,
  Force L3-Learning Port Bounce  = Enabled,
  AP Mode                       = Enabled,
  802.1x Parameters:
          Tx-Period         = 30,
```

```
        Supp-Timeout      = 30,
        Max-reqmeout      = 2
 L2 Profile                    = -,
```

output definitions

Port or **Linkagg ID**	The port or link aggregate on which UNP is enabled. Configured through the **unp port-type** command. A "0" indicates the port is a link aggregate (for example, 0/12 is link aggregate ID 12).
Port Type	The type of UNP port (**Bridge** or **Access**).
Redirect Port Bounce	The status of the port bounce operation (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp redirect port-bounce** command. This field applies only to UNP bridge ports and link aggregates.
802.1x Authentication	The 802.1X authentication status (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp 802.1x-authentication** command.
802.1x Pass Alternate Profile	The name of the 802.1X authentication pass alternate profile assigned to the port or link aggregate. Configured through the **unp 802.1x-authentication pass-alternate** command
802.1x Bypass	The status of 802.1X bypass (**Enabled** or **Disabled**).
802.1x failure-policy	Whether the switch attempts subsequent MAC authentication for a device after the initial 802.1X authentication process fails (**default** = no MAC authentication or **mac-authentication**).
Mac-auth allow-eap	Indicates the conditions under which 802.1X authentication is performed or bypassed based on the initial MAC authentication process (**pass** = MAC authentication passes, **fail** = if MAC authentication fails, **noauth** = no MAC authentication, or **none** = do not attempt 802.1X authentication). This parameter option only applies to a UNP port or link aggregate on which 802.1X authentication bypass is enabled. Configured through the **unp mac-authentication allow-eap** command.
Mac Authentication	The MAC authentication status (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp mac-authentication** command.
Mac Pass Alternate Profile	The name of the MAC authentication pass alternate profile assigned to the port or link aggregate. Configured through the **unp mac-authentication pass-alternate** command.
Classification	The classification status (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp classification** command.
Trust-Tag	The status of the trust VLAN tag option for the UNP port or link aggregate. Configured through the **unp trust-tag** command.
Default Profile	The name of the default UNP profile assigned to the UNP port or link aggregate. Configured through the **unp default-profile** command.
Port Domain Name	The domain ID number assigned to the UNP port or link aggregate. Configured through the **unp domain** command.
AAA Profile	The name of an AAA profile assigned to the UNP port or link aggregate. Configured through the **unp aaa-profile** command.

output definitions

Port Template	The name of a port template assigned to the UNP port or link aggregate. A port template defines and saves UNP port configuration options (such as the type of authentication, classification status, a default profile). Configured through the **unp port port-template** command.
Port Control Direction	Whether 802.1X access control is applied to ingress and egress traffic (**both**) or just ingress traffic (**in**). Configured through the **unp direction** command. This field applies only to UNP bridge ports and link aggregates.
Egress Flooding	Indicates whether egress broadcast, unknown unicast, and multicast traffic is blocked (**Not Allowed**) or unblocked (**Allowed**) on the UNP port. The value displayed in this field is based on the port control direction setting for the port (**both** = Not Allowed; **in** = Allowed). This field is displayed only for UNP bridge ports and link aggregates.
Admin State	The administrative status (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp admin-state** command.
Dynamic Service	The type of dynamic service (**vxlan** or **spb**) to generate on the UNP port or link aggregate. Configured through the **unp dynamic-service** command. This field applies only to UNP access ports and link aggregates.
PVLAN Port Type	The Private VLAN (PVLAN) port type for the UNP port or link aggregate (**promiscuous**, **isl**, **community**, or **isolated**). This field is displayed only for UNP access ports, not link aggregates.
Force L3-Learning	The status of Layer 3 learning (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp force-l3-learning** command.
Force L3-Learning Port Bounce	The status of the port bounce action, which is an optional parameter associated with the Layer 3 learning function. Configured through the **unp force-l3-learning** command.
AP Mode	The Access Point mode status (**Enabled** or **Disabled**) for the UNP port or link aggregate. Configured through the **unp port ap-mode** command. This field applies only to UNP bridge ports and link aggregates.
802.1x Tx-Period	The amount of time, in seconds, before an EAP Request Identity is retransmitted. Configured through the **unp 802.1x-authentication tx-period** command.
802.1x Supp-Timeout	The amount of time, in seconds, the switch waits before timing out an 802.1X user (supplicant) that is attempting to authenticate. Configured through the **unp 802.1x-authentication supp-timeout** command.
802.1x Max-Req	The maximum number of times the switch will retransmit a request for authentication information. Configured through the **unp 802.1x-authentication max-req** command.
L2 Profile	The name of a Layer 2 profile that is assigned to the UNP port or link aggregate. Configured through the **unp l2-profile** command. This field applies only to UNP access ports and link aggregates.

Release History

Release 8.3.1; command was introduced.
Release 8.3.1.R02; “Force L3-Learning” and “Force L3-Learning Port Bounce” fields added.
Release 8.4.1; “L2 Profile” field added.
Release 8.6R1; “AP Mode” field added.

Related Commands

show unp port	Displays the UNP port configuration for the switch.
show unp profile	Displays the UNP configuration for the switch.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDefaultProfileName
   alaDaUNPPortPassAltProfileName
   alaDaUNPPortMacAuthFlag
   alaDaUNPPortClassificationFlag
   alaDaUNPPortTrustTagStatus
   alaDaUNPPortType
   alaDaUNPPort8021XAuthStatus
   alaDaUNPPort8021XTxPeriod
   alaDaUNPPort8021XSuppTimeOut
   alaDaUNPPort8021XMaxReq
   alaDaUNPPortAaaProfile
   alaDaUNPPortRedirectPortBounce
   alaDaUNPPort8021XFailurePolicy
   alaDaUNPPort8021XBypassStatus
   alaDaUNPPortMacAllowEap
   alaDaUNPPortAdminControlledDirections
   alaDaUNPPortAdminControlledOperDirections
   alaDaUNPPort8021XPassAltProfileName
   alaDaUNPPortPortTemplateName
   alaDaUNPPortDomainID
   alaDaUNPPortAdminState
   alaDaUNPPortDynamicService
   alaDaUNPPortPVlanPortType
   alaDaUNPPortL2Profile
   alaDaUNPPortApMode
```

show unp port bandwidth

Displays the bandwidth parameter values applied to a UNP port or link aggregate. These values are optionally assigned through the UNP profile to which a UNP port is associated.

show unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} bandwidth**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **port** or **linkagg** parameter to display information for a specific port or link aggregate ID.
- Bandwidth parameter values are not applied to UNP link aggregates that are assigned to the profile. As a result, this command will always show the bandwidth parameter values as not set for link aggregates.
- The optional bandwidth parameter values are applied when a UNP port is classified into a UNP profile. The profile name is obtained through local classification or returned from the RADIUS server.
- The source from which the bandwidth parameter values was last updated is also included in the display information. The source updates are based on the following conditions:
  - The UNP profile applies the bandwidth values at the time the UNP port is classified into the profile. This overrides any existing QoS bandwidth policies configured on the physical port.
  - QoS bandwidth policies defined in a QoS policy list associated with the profile are applied after the port is classified into the profile. This overrides the profile bandwidth values initially applied.
  - User-configured QoS bandwidth policies are applied after the port is classified into the profile.

Examples

```
The following example shows the default display of UNP rate limit parameters when
no users are learned on the UNP port:

-> show unp port 1/1/11 bandwidth
Port   Port   Type    Max Ingress Ingress BW Ingr BW  Max Egress Egress BW Egress BW Max Ingress Max Egress
       Domain         Bandwidth   Source     profile  Bandwidth  Source    profile   Depth       Depth
------+------+-------+-----------+----------+--------+----------+---------+---------+-----------+----------
1/1/11 0      Bridge  0                      -       0                     -        0           0

The following example shows the UNP rate limit parameters that are applied when
user devices are assigned to a UNP profile that specifies bandwidth parameter
values:
```

```
-> show unp port 1/1/11 bandwidth
Port   Port   Type   Max Ingress Ingress BW Ingr BW   Max Egress Egress BW Egress BW Max Ingress Max Egress
       Domain        Bandwidth   Source     profile   Bandwidth  Source    profile   Depth       Depth
------+------+------+-----------+----------+---------+----------+---------+---------+-----------+----------
1/1/11 0      Bridge 50.0M       UNP        Ingress50 30.0M      UNP       Egress30  0           0
```

The following example shows the rate limit parameter values that are applied when QoS policies override the bandwidth parameter values that were applied through UNP profile settings:

```
-> qos port 1/1/11 maximum ingress-bandwidth 60M maximum egress-bandwidth 60M

-> show unp port 1/1/11 bandwidth
Port   Port   Type   Max Ingress Ingress BW Ingr BW   Max Egress Egress BW Egress BW Max Ingress Max Egress
       Domain        Bandwidth   Source     profile   Bandwidth  Source    profile   Depth       Depth
------+------+------+-----------+----------+---------+----------+---------+---------+-----------+----------
1/1/11 0      Bridge 60.0M       QOS        -         60.0M      QOS       -         0           0
```

output definitions

Port	The port or link aggregate on which UNP is enabled. A “0” indicates the port is a link aggregate (for example, 0/11 is link aggregate ID 11). Configured through the **unp port-type** command.
Port Domain	The domain ID assigned to the UNP port or link aggregate. Configured through the **unp domain** command.
Type	The type of UNP port (**Bridge** or **Access**). Configured through the **unp port-type** command.
Max Ingress Bandwidth	The maximum ingress bandwidth value applied to the UNP port. Configured through the **unp profile maximum-ingress-bandwidth** command.
Ingress BW Source	The source from which the maximum ingress bandwidth value was updated on the port (**UNP** or **QoS**).
Ingr BW Profile	The name of the UNP profile responsible for setting the maximum ingress bandwidth value on the UNP port. This field is only applicable when UNP classification applies the bandwidth setting on the port.
Max Egress Bandwidth	The maximum egress bandwidth value applied to the UNP port. Configured through the **unp profile maximum-egress-bandwidth** command.
Egress BW Source	The source from which the maximum egress bandwidth value was updated on the port (**UNP** or **QoS**).
Egress BW Profile	The name of the UNP profile responsible for setting the maximum egress bandwidth value on the UNP port. This field is only applicable when UNP classification applies the bandwidth setting on the port.
Max Ingress Depth	The maximum ingress depth value that is applied to the UNP port. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. Configured through the **unp profile maximum-ingress-depth** command.
Max Egress Depth	The maximum egress depth value that is applied to the UNP port. This value determines how much the traffic can burst over the maximum egress bandwidth rate. Configured through the **unp profile maximum-egress-depth** command.

Release History

Release 8.2.1; command was introduced.

Related Commands

show unp port	Displays the UNP port configuration for the switch.
show unp profile	Displays the UNP profile configuration for the switch.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortIfIndex
   alaDaUNPPortDomainID
   alaDaUNPPortType
   alaDaUNPPortMaxIngressBw
   alaDaUNPPortMaxIngressBwSource
   alaDaUNPPortMaxEgressBw
   alaDaUNPPortMaxEgressBwSource
   alaDaUNPPortMaxIngressDepth
   alaDaUNPPortMaxEgressDepth
   alaDaUNPPortIngressSourceProfile
   alaDaUNPPortEgressSourceProfile
```

show unp port 802.1x statistics

Displays 802.1X statistics for a UNP port or link aggregate on which 802.1X authentication is enabled.

show unp {port *chassis/slot/port1***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} 802.1x statistics**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID. Use a hyphen to specify a range of link aggregates IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **port** or **linkagg** parameter to display information for a specific UNP port or link aggregate ID.

Examples

```
-> show unp port 1/1/13 802.1x statistics
Port  1/1
    Mac-address=00:00:00:00:00:01,
        Vlan=0,
          Rx EAP Frames=0,
          Tx EAP Frames=0,
          Rx EAP Logoff Frames=0,
          Tx EAP Request Frames=0,
          Tx EAP Request ID Frames=0,
          Rx EAP Response Frames=0,
          Rx EAP Response ID Frames=0,
          Rx EAP Start Frames=0,
          Rx Invalid EAP Frames=0,
          Rx Length Error EAP Frames=0,
          Last EAP Frame Version=0,
          Last EAP Frame Version=0,
          Last EAP Source=00:00:00:00:00:00
```

```
-> show unp linkagg 20 802.1x statistics
Linkagg ID 0/10
    Mac-address=00:00:00:00:00:01,
        Vlan=0,
          Rx EAP Frames=0,
          Tx EAP Frames=0,
          Rx EAP Logoff Frames=0,
          Tx EAP Request Frames=0,
          Tx EAP Request ID Frames=0,
          Rx EAP Response Frames=0,
          Rx EAP Response ID Frames=0,
          Rx EAP Start Frames=0,
          Rx Invalid EAP Frames=0,
          Rx Length Error EAP Frames=0,
          Last EAP Frame Version=0,
          Last EAP Frame Version=0,
          Last EAP Source=00:00:00:00:00:00
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show unp port	Displays the UNP port configuration for the switch.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

N/A

show unp port configured-vlans

Displays the VLANs assigned to UNP bridge ports or link aggregates.

show unp {port [*chassis/slot/port1***[-***port2***]] | linkagg [***agg_id***[-***agg_id2***]} configured-vlans**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP bridge port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID for a specific UNP bridge link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **port** or **linkagg** parameter to display information for a specific UNP bridge port or link aggregate ID.
- If the **port** or **linkagg** parameter is used without specifying an individual port, a range of ports, or link aggregate ID, then the configured VLAN information for all UNP ports and link aggregates is displayed.
- The “Type” field indicates if the VLAN assignment is untagged (unpUntag) or tagged (unpQtag).

Examples

```
-> show unp port configured-vlans
Port     Vlan   Type
-------+------+---------
0/10      500  unpUntag
0/10      501  unpUntag
1/1/10    600  unpQtag
1/1/11    601  unpUntag
1/1/11    602  unpQtag
1/1/11    603  unpQtag

-> show unp port 1/1/11 configured-vlans
Port     Vlan   Type
-------+------+---------
1/1/11    601  unpUntag
1/1/11    602  unpQtag
1/1/11    603  unpQtag
```

```
-> show unp linkagg configured-vlans
LagId    Vlan   Type
-------+------+---------
0/10      500  unpUntag
0/10      501  unpQtag
0/100     100  unpQtag
0/100     101  unpUntag
0/101     200  unpQtag
0/101     201  unpQtag

-> show unp linkagg 100 configured-vlans
LagId    Vlan   Type
-------+------+---------
0/100     100  unpQtag
0/100     101  unpUntag
```

Release History

Release 8.2.1; command was introduced.
Release 8.5R4; **Type** field added.

Related Commands

unp vlan	Configures VLAN assignments for UNP bridge ports.
show unp port	Displays the UNP port and link aggregate configuration for the switch.

MIB Objects

```
alaDaUNPPortVlanTable
   alaDaUNPPortVlanVID
```

show unp port profile

Displays the UNP service profiles that are statically assigned to UNP ports or link aggregates.

show unp {port [*chassis/slot/port1***[-***port2***]] | linkagg [***agg_id***[-***agg_id2***]} profile**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
*agg_id***[-***agg_id2***]**	Link aggregate ID for a specific UNP link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **port** or **linkagg** parameter to display information for a specific UNP port or link aggregate ID.
- If the **port** or **linkagg** parameter is used without specifying an individual port, a range of ports, or link aggregate ID, then the static profile information for all UNP ports and link aggregates is displayed.

Examples

```
-> show unp port profile
Port    Profile
-------+----------------
1/1/5   static-spb1
1/1/5   static-spb2
1/1/10  static-vxlan1
1/1/10  static-vxlan2
1/1/20  static-l2gre

-> show unp port 1/1/5 profile
Port    Profile
-------+----------------
1/1/5   static-spb1
1/1/5   static-spb2
```

Release History

Release 8.5R4; command was introduced.

Related Commands

unp port profile	Configures static profile assignments for UNP ports.
show unp port	Displays the UNP port and link aggregate configuration for the switch.

MIB Objects

```
alaDaUNPPortTable
   alaDaUNPPortProfile
```

show unp port-template

Displays the port template configuration for the switch.

show unp port-template [*template_name***] [config | configured-vlans | profile]**

Syntax Definitions

template_name	The name of the UNP port template to display.
config	Displays additional details about the parameter configuration for the template.
configured-vlans	Displays the VLAN IDs that the specified template assigns to a UNP port.
profile	Displays the names of UNP service profiles that the specified template assigns as static profiles to a UNP port.

Defaults

By default, displays a summary of the configuration information for all port templates.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Enter a template name with this command to display information for a specific port template.
- Use the **config** option with this command to display the full configuration for each template.
- Use the **configured-vlans** option with this command to display the VLAN IDs that a port template will statically assign to a UNP bridge port when the template is applied on the port. Configuring a static VLAN-port association (VPA) applies only to UNP bridge ports.
- Use the **profile** option with this command to display the names of UNP service profiles that a port template will assign as a static profile to a UNP port when the template is applied on the port.

Examples

```
-> show unp port-template
                                802.1x                    Mac-Auth         Redirect
Template Name            802.1x   Pass-Alt Profile Mac-Auth Pass-Alt Profile Port-Bounce Class.   Trust-Tag
-------------------------+--------+----------------+--------+----------------+-----------+--------+---------
unp-port1                 Enabled   1xPass         Disabled   -              Disabled    Disabled Disabled
unp-port2                 Disabled  -              Enabled    macPass        Disabled    Enabled  Enabled
accessDefaultPortTemplate Enabled   -              Enabled    -              Disabled    Enabled  Enabled
bridgeDefaultPortTemplate Enabled   -              Enabled    -              Disabled    Enabled  Enabled

Total Port-Template Count: 4

-> show unp port-template unp-port2
                                802.1x                    Mac-Auth         Redirect
Template Name            802.1x   Pass-Alt Profile Mac-Auth Pass-Alt Profile Port-Bounce Class.   Trust-Tag
-------------------------+--------+----------------+--------+----------------+-----------+--------+---------
unp-port2                 Disabled  -              Enabled    macPass        Disabled    Enabled  Enabled
```

```
-> show unp port-template accessDefaultPortTemplate
                              802.1x                   Mac-Auth         Redirect
Template Name           802.1x   Pass-Alt Profile Mac-Auth Pass-Alt Profile Port-Bounce Class.   Trust-Tag
------------------------+--------+---------------+--------+---------------+-----------+--------+---------
accessDefaultPortTemplate Enabled   -              Enabled    -              Disabled    Enabled  Enabled

-> show unp port-template port-2 config

Port Template: unp-port2
  802.1x Authentication           = Disabled,
  802.1x Pass Alternate Profile   = -,
  Mac Authentication              = Enabled,
  Mac-Auth Pass Alternate Profile = macPass,
  Classification                  = Enabled,
  Trust-tag                       = Enabled,
  Default Profile                 = -,
  Port Domain Number              = 0,
  AAA-Profile                     = ,
  Redirect Port Bounce            = Disabled,
  Port Control Direction          = Both,
  802.1x Tx-Period                = 0,
  802.1x Supp-Timeout             = 0,
  802.1x Max-Req                  = 2,
  802.1x Bypass                   = Disabled,
  802.1x failure-policy           = default,
  Mac-auth allow-eap              = -,
  Force L3-Learning               = Disabled
  Force L3-Learning Port Bounce   = Disabled
  Admin State                     = Enabled,
  Dynamic Service                 = -,
  L2 Profile                      = -,
  AP Mode                         = Enabled,

-> show unp port-template accessDefaultPortTemplate config

Port Template: accessDefaultPortTemplate
  802.1x Authentication           = Enabled,
  802.1x Pass Alternate Profile   = -,
  Mac Authentication              = Enabled,
  Mac-Auth Pass Alternate Profile = -,
  Classification                  = Enabled,
  Trust-tag                       = Enabled,
  Default Profile                 = -,
  Port Domain Num                 = 0,
  Redirect Port Bounce            = Disabled,
  AAA Profile                     = -,
  Port Control Direction          = Both,
  802.1x Tx-Period                = 30,
  802.1x Supp-Timeout             = 30,
  802.1x Max-Req                  = 2,
  802.1x Bypass                   = Disabled,
  802.1x failure-policy           = default,
  Mac-auth allow-eap              = -,
  Force L3-Learning               = Disabled
  Force L3-Learning Port Bounce   = Enabled
  Admin State                     = Enabled,
  Dynamic Service                 = spb,
  L2 Profile                      = "unp-def-access-profile",
  AP Mode                         = -,
```

output definitions

Port Template	The name of the port template. By default, the "accessDefaultPortTemplate" is assigned to UNP access ports and the "bridgeDefaultPortTemplate" is assigned to UNP bridge ports.
802.1x Authentication	The 802.1X authentication status (**Enabled** or **Disabled**).
802.1x Pass Alternate Profile	The name of an alternate profile for devices that pass 802.1X authentication.
Mac Authentication	The MAC authentication status (**Enabled** or **Disabled**).
Mac-Auth Pass Alternate Profile	The name of an alternate profile for devices that pass MAC authentication.
Classification	The classification status (**Enabled** or **Disabled**).
Trust-Tag	The trust VLAN ID tag status (**Enabled** or **Disabled**).
Default Profile	The name of a default profile for devices that are not classified by any other classification methods.
Port Domain Num	The domain ID number assignment for the UNP port.
Redirect Port Bounce	The status of port bounce (**Enabled** or **Disabled**) for BYOD registration and authorization.This parameter is only configurable on UNP bridge ports.
AAA Profile	The name of an AAA profile to apply to the port.
Port Control Direction	Whether 802.1X access control is applied to ingress and egress traffic (**both**) or just ingress traffic (**in**). This parameter is only configurable on UNP bridge ports.
802.1x Tx-Period	The amount of time, in seconds, before an EAP Request Identity is retransmitted.
802.1x Supp-Timeout	The amount of time, in seconds, the switch will wait before timing out an 802.1X user that is attempting to authenticate.
802.1x Max-Req	The maximum number of times the switch will retransmit a request for authentication information.
802.1x Bypass	The status of 802.1X bypass (**Enabled** or **Disabled**).
802.1x failure-policy	Whether the switch attempts subsequent MAC authentication for a device after the initial 802.1X authentication process fails (**default** = no MAC authentication is attempted or **mac-authentication**).
Mac-auth allow-eap	The conditions under which 802.1X authentication is performed or bypassed based on the initial MAC authentication process (**pass** = if MAC authentication passes, **fail** = if MAC authentication fails, or **noauth** = if MAC authentication is not configured). This parameter option only applies to UNP ports on which 802.1X authentication bypass is enabled.
Force L3-Learning	The status of Layer 3 learning (**Enabled** or **Disabled**).
Force L3-Learning Port Bounce	The status of the port bounce action, which is an optional parameter associated with the Layer 3 learning function.
Admin State	The administrative status of the UNP port configuration (**Enabled** or **Disabled**).
Dynamic Service	Whether the UNP port generates dynamic SPB or VXLAN services. This parameter is only configurable on UNP access ports.

output definitions

L2 Profile	The name of a Layer 2 service profile to apply to a UNP access port. This parameter is not configurable when the template is assigned to a UNP bridge port.
AP Mode	The status of Access Point (AP) mode functionality (**Enabled** or **Disabled**). This parameter is only configurable on UNP bridge ports.

```
-> show unp port-template unp-pt1 configured-vlans
Template Name                    Vlan  Type
-------------------------------+------+----------
unp-pt1                          200   unpUntag
unp-pt1                          201   unpQtag
```

output definitions

Template Name	The name of a UNP port template.
VLAN	The VLAN IDs that are assigned to a UNP bridge port when the template is applied to the port.
Type	Indicates if the VLAN assignment is untagged (**unpUntag**) or tagged (**unpQtag**).

```
-> show unp port-template unp-port1 profile
Template Name                   Profile
-------------------------------+----------------
unp-port1                        static-spb1
                                 static-spb2
```

output definitions

Template Name	The name of a UNP port template.
Profile	The name of UNP service profiles that are statically assigned to a UNP port when the template is applied to the port.

Release History

Release 8.3.1; command was introduced.
Release 8.3.1.R02; “Force L3-Learning” and “Force L3-Learning Port Bounce” fields added.
Release 8.4.1; “L2 Profile” field added.
Release 8.5R4; **profile** parameter added, “Type” field added to configured VLANs display.
Release 8.6R1; “AP Mode” field added.

Related Commands

unp port-template	Configures UNP port parameter values for a port template.
unp port port-template	Assigns a port configuration template to a UNP port.
show unp port config	Displays the full UNP configuration for a port, including the name of a port template that is associated with the port.

MIB Objects

```
alaDaUNPPortTemplateTable
   alaDaUNPPortTemplateName
   alaDaUNPPortTemplateAdminState
   alaDaUNPPortTemplateDirection
   alaDaUNPPortTemplateDomainID
   alaDaUNPPortTemplateClassification
   alaDaUNPPortTemplateTrustTag
   alaDaUNPPortTemplateDynamicService
   alaDaUNPPortTemplateDefaultProfile
   alaDaUNPPortTemplateAAAProfile
   alaDaUNPPortTemplateRedirectPortBounce
   alaDaUNPPortTemplate8021XAuth
   alaDaUNPPortTemplate8021XAuthPassAlternate
   alaDaUNPPortTemplate8021XAuthBypass
   alaDaUNPPortTemplate8021XAuthFailPolicy
   alaDaUNPPortTemplate8021XAuthTxPeriod
   alaDaUNPPortTemplate8021XAuthSuppTimeout
   alaDaUNPPortTemplate8021XAuthMaxReq
   alaDaUNPPortTemplateMACAuth
   alaDaUNPPortTemplateMACAuthPassAlternate
   alaDaUNPPortTemplateMACAuthAllowEAP
   alaDaUNPPortTemplateForceL3Learning
   alaDaUNPPortTemplateForceL3LearningPortBounce
   alaDaUNPPortTemplateL2Profile
   alaDaUNPPortTemplateApMode
alaDaUNPPortTemplateVlanTable
   alaDaUNPPortTemplateVlanVID
alaDaUNPPortTemplateProfileTable
   alaDaUNPPortTemplateProfile
```

show unp user

Displays information about the MAC addresses learned on a UNP port or link aggregate.

show unp user [port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]] [sap-id** *sap_id***] [service-id** *service_id***] [profile** *profile_name***] [authentication-type {none | mac | 802.1x}] [mac-address** *mac_address***] [count]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8). This parameter displays all UNP users learned on the specified port number.
*agg_id***[**-*agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15). This parameter displays all UNP users learned on the specified link aggregate ID.
sap_id	A Service Access Point (SAP) ID. This parameter displays all UNP users associated with the specified SAP ID.
service_id	A service ID number. This parameter displays all UNP users associated with the specified service ID.
profile_name	The name of an existing UNP profile. This parameter displays all UNP users associated with the specified profile name.
none	Displays all UNP users that did not undergo the authentication process.
mac	Displays all UNP users that were authenticated through the MAC authentication process.
802.1x	Displays all UNP users that were authenticated through the 802.1X authentication process.
mac_address	A source MAC address. This parameter displays the UNP user device with the specified source MAC address.
count	Displays the number of UNP users learned on the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the optional parameters provided with this command to filter the output display results. In addition, some parameters can be combined to further narrow the display results. For example:
  - Combine the **port** or **linkagg** parameter with the **profile** parameter option to display users learned on the port or link aggregate that are classified into the specified profile.
  - Combine the **port** or **linkagg** parameter with the **authentication-type** parameter option to display users on the port or link aggregate that were authenticated with the specified authentication type.

- The “Username” field displays the user name that was entered to authenticate an 802.1X user device or the user name that was entered to successfully authenticate a user device through the Captive Portal process. However, if a user device first undergoes 802.1X authentication and then undergoes successful Captive Portal authentication, the user name entered during the Captive Portal process is displayed in this field.

Examples

```
-> show unp user count
Total users: 6

-> show unp user
                                          User
Port  Username           Mac address      IP      Vlan Profile   Type    Status
-----+------------------+----------------+-------+----+---------+-------+-------
1/1/1 00:00:00:00:00:01  00:00:00:00:00:01  1.1.1.1  10  unp-1     Access  Active
1/1/2 00:00:00:00:00:02  00:00:00:00:00:02  1.1.1.2  11  unp-2     Bridge  Active
1/1/3 guest_user         00:00:00:00:00:04  1.1.1.4  20  unp-guest Access  Active
1/1/7 00:00:00:00:00:07  00:00:00:00:00:07  1.1.1.7  11  unp-emp   Bridge  Active
0/10  Employee-001       00:00:00:00:00:03  1.1.1.3  12  unp-emp   Bridge  Active
0/12  00:00:00:00:00:14  00:00:00:00:00:14  1.1.2.4  20  unp-7     Bridge  Active

Total users : 6
```

output definitions

Port	The port or link aggregate on which the MAC address was learned. A “0” indicates the UNP port is a link aggregate (e.g., 0/10 refers to link aggregate ID 10).
Username	Displays either a source MAC address or a Captive Portal user name for the learned user device.
MAC address	The MAC address of the user device. This field and the **Username** field may contain the same MAC address, depending on how the user device was authenticated.
User IP	The IP network address of the user device.
Vlan	The UNP VLAN ID to which the user device was assigned. This only applies for users authenticated into VLAN profiles.
Profile	The name of the UNP profile to which the user device was assigned.
Type	The type of UNP port on which the device was learned (**Bridge** or **Access**).
Status	The status of the device: • **In progress**—device learning is in progress. • **Active**—device is learned in forwarding state. • **Block**—device is learned in filtering state.

```
-> show unp user port 1/1/3
                                          User
Port   Username           Mac address      IP      Vlan  Profile     Auth   Role
------+------------------+----------------+-------+-----+-----------+------+------
1/1/3  guest_user         00:00:00:00:00:04 1.1.1.4  20   unp-guest   8021X  Guest

Total users : 1
```

```
-> show unp user linkagg 10
                                          User
Port   Username           Mac address     IP      Vlan  Profile     Auth   Role
------+-----------------+----------------+-------+-----+-----------+-----+--------
0/10   Employee-001      00:00:00:00:00:03 1.1.1.3  12   unp-emp     8021X Employee

Total users : 1

-> show unp user profile unp-emp
                                          User
Port   Username           Mac address     IP      Vlan  Profile     Auth   Role
------+-----------------+----------------+-------+-----+-----------+-----+--------
1/1/7  00:00:00:00:00:07 00:00:00:00:00:07 1.1.1.7  11   unp-emp     MAC   Employee
0/10   Employee-001      00:00:00:00:00:03 1.1.1.3  12   unp-emp     8021X Employee

Total users : 2

-> show unp user authentication-type mac
                                          User
Port   Username           Mac address     IP      Vlan  Profile     Auth   Role
------+-----------------+----------------+-------+-----+-----------+-----+--------
1/1/7  00:00:00:00:00:07 00:00:00:00:00:07 1.1.1.7  11   unp-emp     MAC   Employee
0/12   00:00:00:00:00:14 00:00:00:00:00:14 1.1.2.4  20   unp-7       MAC   Employee

Total users : 2
```

output definitions

Port	The port or link aggregate on which the MAC address was learned. A “0” indicates the UNP port is a link aggregate (e.g., 0/10 refers to link aggregate ID 10).
Username	Displays either a source MAC address or a Captive Portal user name for the learned user device.
MAC address	The MAC address of the user device. This field and the **Username** field may contain the same MAC address, depending on how the user device was authenticated.
User IP	The IP network address of the user device.
Vlan	The UNP VLAN ID to which the user device was assigned. This only applies for users authenticated into VLAN profiles.
Profile	The name of the UNP profile to which the user device was assigned.
Auth	The type of authentication applied to the user (**none**, **mac**, or **802.1X**).
Role	The user role (QoS policy list) applied to the user device.

Release History

Release 8.1.1; command was introduced.

Related Commands

show unp user status	Displays information about the authentication and validation status of users learned on UNP ports.
show unp user details	Displays detailed information about user devices learned on UNP ports.
unp user flush	Performs a MAC address flush of Access Guardian users (devices learned on UNP ports).
show zeroconf server policy-instances	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

N/A

show unp user status

Displays the status of the authentication and validation process for MAC addresses learned on a UNP port or link aggregate.

show unp user status [port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***] [sap-id** *sap_id***] [service-id** *service_id***] [profile** *profile_name***] [authentication-type {none | mac | 802.1x}] [mac-address** *mac_address***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	Link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (10-15).
sap_id	A Service Access Point (SAP) ID. This parameter displays all UNP users associated with the specified SAP ID.
service_id	A service ID number. This parameter displays all UNP users associated with the specified service ID.
profile_name	The name of an existing UNP profile.
none	Displays users that did not undergo the authentication process.
mac	Displays users that were authenticated through MAC authentication.
802.1x	Displays users that were authenticated through 802.1X authentication.
mac_address	The user device MAC address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the optional parameters provided with this command to filter the output display results. In addition, some parameters can be combined to further narrow the display results. For example:

- Combine the **port** or **linkagg** parameter with the **profile** parameter option to display users learned on the port or link aggregate that are classified into the specified profile.
- Combine the **port** or **linkagg** parameter with the **authentication-type** parameter option to display users on the port or link aggregate that were authenticated with the specified authentication type.

Examples

```
-> show unp user status port 1/1/1
                       Profile  Profile Authentication Role  Role                Restricted
Port  Mac address       Name     Source  Type   Status  Name  Source  CP  Redirect Access
-----+-----------------+--------+-------+------+-------+-----+-------+---+--------+----------
1/1/1 00:00:00:00:00:05 Prf1     Radius  8021x  Passed  emp1  Profile  Y  -        -

Total users : 1

-> show unp user status linkagg 100
                       Profile  Profile Authentication Role  Role                Restricted
Port  Mac address       Name     Source  Type   Status  Name  Source  CP  Redirect Access
-----+-----------------+--------+-------+------+-------+-----+-------+---+--------+----------
0/100 00:00:00:00:00:06 Prf3     Radius  8021x  Passed  emp1  Profile  Y  -        -

Total users : 1

-> show unp user status authentication type MAC
                       Profile  Profile Authentication Role  Role                Restricted
Port  Mac address       Name     Source  Type   Status  Name  Source  CP  Redirect Access
-----+-----------------+--------+-------+------+-------+-----+-------+---+--------+----------
1/1/2 00:00:00:00:00:15 Prf2     Alt     MAC    Passed  emp2  Profile  Y  -        -

Total users : 1
```

output definitions

Port	The port or link aggregate on which the MAC address was learned. A “0” indicates the UNP port is a link aggregate (e.g., 0/10 refers to link aggregate ID 10).
MAC address	The MAC address of the user device.
Profile Name	The name of the UNP to which the user device was assigned.
Profile Source	The source of the profile assignment (e.g., Radius, Alt).
Authentication Type	The type of authentication applied to the user (**none**, **mac**, or **802.1X**).
Authentication Status	The authentication status for the device.
Role Name	The name of the user role applied to the user device.
Role Source	The source of the user role applied to the user device.
CP	Indicates if the device was authenticated through Captive Portal.
Redirect	The redirection status.
Restricted Access	Whether or not access is restricted for the user.

Release History

Release 8.1.1; command was introduced.

Related Commands

show unp user	Displays information about users learned on a UNP ports.
show unp user details	Displays detailed information about users learned on a UNP ports.
show zeroconf server policy-instances	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

N/A

show unp user details

Displays additional details about the MAC addresses learned on a UNP port or link aggregate.

show unp user details [port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]] [sap-id** *sap_id***] [service-id** *service_id***] [profile** *profile_name***] [authentication-type {none | mac | 802.1x}] [mac-address** *mac_address***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8). This parameter displays all UNP users learned on the specified port number.
*agg_id***[-***agg_id2***]**	Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15). This parameter displays all UNP users learned on the specified link aggregate ID.
sap_id	A Service Access Point (SAP) ID. This parameter displays all UNP users associated with the specified SAP ID.
service_id	A service ID number. This parameter displays all UNP users associated with the specified service ID.
profile_name	The name of an existing UNP profile. This parameter displays all UNP users associated with the specified profile name.
none	Displays all UNP users that did not undergo the authentication process.
mac	Displays all UNP users that were authenticated through the MAC authentication process.
802.1x	Displays all UNP users that were authenticated through the 802.1X authentication process.
mac_address	A source MAC address. This parameter displays the UNP user device with the specified source MAC address.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the optional parameters provided with this command to filter the output display results. In addition, some parameters can be combined to further narrow the display results. For example:
  - Combine the **port** or **linkagg** parameter with the **profile** parameter option to display users learned on the port or link aggregate that are classified into the specified profile.
  - Combine the **port** or **linkagg** parameter with the **authentication-type** parameter option to display users on the port or link aggregate that were authenticated with the specified authentication type.

- The “User Name” field displays the user name that was entered to authenticate an 802.1X user device or the user name that was entered to successfully authenticate a user device through the Captive Portal process. However, if a user device first undergoes 802.1X authentication and then undergoes successful Captive Portal authentication, the user name entered during the Captive Portal process is displayed in this field.

Examples

```
-> show unp user details port 1/1/10

Port:  1/1/10
  MAC-Address: 00:00:00:00:00:01
Sap                             : -,
Service ID                      : -,
VNID                            : -,
ISID                            : -,
VPNID                           : 200,
Access Timestamp                : 04/01/1970 18:45:26,
User Name                       : guest1,
IP-address                      : 10.0.0.1,
Vlan                            : 10,
Authentication Type             : 802.1X,
Authentication Status           : Authenticated,
Authentication Failure Reason   : -,
Authentication Retry Count      : -,
Authentication Server IP Used   = 10.135.62.129,
Authentication Server Used      = rad1,
Server Reply-Message            = -,
Profile                         : Employee,
Profile Source                  : RADIUS Server Profile,
Profile From Auth Server        : Employee,
Classification profile rule     : -,
Role                            : Employee,
Role Source                     : Profile,
User role rule                  : -,
Restricted Access               : No,
Location Policy Status          : Passed,
Time Policy Status              : Passed,
Captive-Portal Status           : -,
QMR Status                      : Passed,
Redirect Url                    : -,
SIP Call Type                   = Not in a call,
SIP Media Type                  = None,
Applications                    = None

  MAC-Address: 00:00:00:00:00:02
Sap                             : -,
Service ID                      : -,
VNID                            : -,
ISID                            : -,
VPNID                           : 200,
Access Timestamp                : 06/01/1989 20:45:26,
User Name                       : guest2,
IP-address                      : 20.0.0.1,
Vlan                            : 20,
Authentication Type             : MAC,
Authentication Status           : Authenticated,
Authentication Failure Reason   : -,
```

```
Authentication Retry Count      : -,
Authentication Server IP Used   = 10.135.62.129,
Authentication Server Used      = rad1,
Server Reply-Message            = -,
Profile                         : Contractor,
Profile Source                  : RADIUS Server Profile,
Profile From Auth Server        : Contractor,
Classification profile rule     : -,
Role                            : Contractor,
Role Source                     : Profile,
User role rule                  : -,
Restricted Access               : No,
Location Policy Status          : Passed,
Time Policy Status              : Passed,
Captive-Portal Status           : Passed,
QMR Status                      : -,
Redirect Url                    : -,
SIP Call Type                   = Normal Call,
SIP Media Type                  = Video,
Applications                    = None

-> show unp user details linkagg 100
Port:  0/100
  MAC-Address: 00:00:00:00:00:03
Sap                             : -,
Service ID                      : -,
VNID                            : -,
ISID                            : -,
VPNID                           : 200,
Access Timestamp                : 02/01/2013 20:45:26,
User Name                       : guest3,
IP-address                      : 30.0.0.1,
Vlan                            : 30,
Authentication Type             : MAC,
Authentication Status           : Authenticated,
Authentication Failure Reason   : -,
Authentication Retry Count      : -,
Authentication Server IP Used   = 10.135.62.129,
Authentication Server Used      = rad1,
Server Reply-Message            = -,
Profile                         : Contractor,
Profile Source                  : Auth - Pass - Default UNP,
Profile From Auth Server        : Employee [Not Configured],
Classification profile rule     : -,
Role                            : Contractor,
Role Source                     : Profile,
User role rule                  : -,
Restricted Access               : No,
Location Policy Status          : Passed,
Time Policy Status              : Passed,
Captive-Portal Status           : Passed,
QMR Status                      : -,
Redirect Url                    : -,
SIP Call Type                   = Not in a call,
SIP Media Type                  = None,
Applications                    = ;Facebook;rediff;
```

output definitions

Port	The UNP port or link aggregate on which the device was learned.
Mac-address	The MAC address of the device.
SAP	The port or link aggregate and encapsulation value for an SPB or VXLAN Service Access Point (SAP).
Service ID	The SPB or VXLAN service ID number.
VNID	The VXLAN Network Identifier. This value is associated with a VXLAN service ID.
ISID	The SPB service instance identifier. This value is associated with an SPB service ID.
VPNID	The L2 GRE tunnel VPN ID.
Access Timestamp	The date and time the device was learned.
User Name	The MAC address of the user.
IP-Address	The IP network address of the device.
Vlan	The VLAN ID number for the VLAN in which the device was learned.
Authentication Type	The type of authentication used (**Mac-Authentication** or **802.1x-Authentication**).
Authentication Status	The status of the authentication process (**blank** "–", **Authenticated**, **Failed**, or **In Progress**).
Authentication Failure Reason	The reason authentication failed.
Authentication Retry Count	The number of times authentication has been attempted.
Authentication Server IP Used	The IP address of the authentication server.
Authentication Server Used	The name of the authentication server used.
Server Reply-Message	Reply message from the authentication server.
Profile	The name of the UNP profile to which the user was assigned.
Profile Source	The source of the profile (returned from the server or assigned through the UNP process on the switch).
Profile From Auth Server	The name of the UNP profile returned from the authentication server.
Classification profile rule	The rule that resulted in the device classification into the UNP profile.
QMR Status	The Quarantine Manager Remediation status for the device.
Redirect Url	The URL to which the device is redirected upon classification.
SIP Call Type	The Session Initiation Protocol (SIP) call type status for a non-supplicant (non-802.1X) device.
SIP Media Type	The SIP media type status for a non-supplicant device.
Applications	The applications a non-supplicant device is running.

Release History

Release 8.1.1; command was introduced.
Release 8.4.1.R02; **VPNID** field added.

Related Commands

show unp user status	Displays information about the authentication and validation status of users learned on UNP ports.
unp user flush	Performs a MAC address flush of Access Guardian users (devices learned on UNP ports).
show zeroconf server policy-instances	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

N/A

show unp policy validity-period

Displays the UNP period policy configuration for the switch. This type of policy is assigned to a UNP profile and applied to devices classified into the profile.

show unp policy validity-period [*policy_name***]**

Syntax Definitions

policy_name	The name of an existing UNP period policy.

Defaults

By default, all UNP period policies are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enter a UNP period policy name to display information about a specific policy.

Examples

```
-> show unp policy validity-period
Policy Days    Months       Hours         Interval                          TZ Active
------+-------+------------+-------------+---------------------------------+---+----
tp1    SMTWTFS JFMAMJJASOND 08:00 - 17:00            - - -                 -   NO
tp2    ------- ------------     - - -     01/01/13 00:00 - 01/02/13 00:00 CST NO

Total Period Policy Count: 2

-> show unp policy validity-period tp1
Policy Days    Months       Hours         Interval                          TZ Active
------+-------+------------+-------------+---------------------------------+---+----
tp1    SMTWTFS JFMAMJJASOND 08:00 - 17:00              - - -               -   NO
```

Release History

Release 8.1.1; command introduced.

Related Commands

unp policy validity-period	Configures a UNP period policy.
unp profile period-policy	Assigns a UNP period policy to a UNP profile.

MIB Objects

```
alaDaUNPValidityPeriodTable
   alaDaUNPValidityPeriodName
   alaDaUNPValidityPeriodDays
   alaDaUNPValidityPeriodDaysStatus
   alaDaUNPValidityPeriodMonths
   alaDaUNPValidityPeriodMonthsStatus
   alaDaUNPValidityPeriodHour
   alaDaUNPValidityPeriodHourStatus
   alaDaUNPValidityPeriodEndHour
   alaDaUNPValidityPeriodInterval
   alaDaUNPValidityPeriodIntervalStatus
   alaDaUNPValidityPeriodEndInterval
   alaDaUNPValidityPeriodTimezone
   alaDaUNPValidityPeriodTimezoneStatus
   alaDaUNPValidityPeriodActiveStatus
```

show unp policy validity-location

Displays the UNP location policy configuration for the switch. This type of policy is assigned to a UNP profile and applied to devices classified into the profile.

show unp policy validity-location [*policy_name***]**

Syntax Definitions

policy_name	The name of an existing UNP location policy.

Defaults

By default, all UNP location policies are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enter a location policy name to display information about a specific policy.

Examples

```
-> show unp policy validity location
Policy: l1
  Port            = 1/1
  System Name     = shasta
  System Location = Bangalore

Total Location Policy Count: 1
```

Release History

Release 8.1.1; command introduced.

Related Commands

unp policy validity-location	Configures a UNP location policy.
unp profile location-policy	Assigns a UNP location policy to a UNP profile.

MIB Objects

```
alaDaUNPLocationPolicyTable
   alaDaUNPLocationPolicyName
   alaDaUNPLocationPolicyPort
   alaDaUNPLocationPolicyPortHigh
   alaDaUNPLocationPolicyPortStatus
   alaDaUNPLocationPolicySystemName
   alaDaUNPLocationPolicySystemLocation
```

device-profile admin-state

Enables or disables the Device Profiling configuration on the switch.

device-profile admin-state {enable | disable}

Syntax Definitions

enable	Enables Device Profiling configuration on the switch.
disable	Disables Device Profiling configuration on the switch.

Defaults

By default Device Profiling configuration is disabled globally on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When Device Profiling is globally enabled for the switch, Device Profiling functionality is automatically enabled on all ports and link aggregates.

Example

```
-> device-profile admin-state enable
-> device-profile admin-state disable
```

Release History

Release 8.5R2; command was introduced.

Related Commands

device-profile port linkagg	Enables or disables the Device Profiling on the ports or linkagg interface.
show device-profile config	Displays the global configuration of the Device Profile.

MIB Objects

```
alaDpAdminState
```

device-profile port linkagg

Enables or disables the Device Profiling on the ports or linkagg interface.

device-profile [port *chassis/]slot/port1***[-***port2***] | linkagg** *agg_id1***[-***agg_id2***] admin-state {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port1***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id1***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (5-10).
enable	Enables the Device Profiling on the specified port or linkagg.
disable	Disables the Device Profiling on the specified port or linkagg.

Defaults

By default Device Profiling is enabled on all ports or linkagg when the Device Profiling feature is enabled globally on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to disable Device Profiling on specific ports or linkagg when the Device Profiling is globally enabled on the switch.
- Device Profiling configuration is not allowed on VFL or HiGig ports.

Example

```
-> device-profile linkagg 1 admin-state enable
-> device-profile port 2/1/2-5 admin-state enable
-> device-profile port 1/1/2 admin-state enable
-> device-profile port 1/1/2 admin-state disable
-> device-profile linkagg 1-5 admin-state disable
```

Release History

Release 8.5R2; command was introduced.

Related Commands

show device-profile config	Displays the global configuration of the Device Profile.
show device-profile catalog	Displays the details of known and unknown devices identified in the network.

MIB Objects

```
alaDpIfTable
   alaDpIfAdminStatus
```

device-profile device-type

Adds or removes a new device type and category in the Device Profile.

device-profile device-type *type_name* **device-name** *device_name* **from {mac-address** *mac_address* **| dhcp-option-55** *dhcp_option***}**

no device-profile device-type *type_name*

Syntax Definitions

type_name	The type of the device. The device type name can be of maximum size 32 alphanumeric characters.
device_name	The name of the device type. The device name can be of maximum size 32 alphanumeric characters.
mac_address	The MAC address of the device. The device with that MAC address must be in the unknown cataloged devices.
dhcp_option	The DHCP option 55 codes of the device.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The unknown cataloged devices can be identified or moved to trusted identity in the Device Profile using this command.
- While specifying the MAC address of the device for identity, the device must first be present in the unknown cataloged devices. Otherwise, the MAC address will not be recognized.
- Custom signatures can be created using the DHCP option 55.
- The new signatures created will not be persistent unless it is saved. Use the **device-profile update-signature** CLI command to update the flash or signature database.
- Use the **no** form of the command to remove the device and its category from the trusted device list.

Example

```
-> device-profile device-type Printer-Fax device-name Kyocera-Printer mac-address
00:aa:bb:12:43:55
-> device-profile device-type IP-Camera device-name netgear dhcp-option-55
1,3,6,15,119,252
-> no device-profile device-type Printer-Fax
```

Release History

Release 8.5R2; command was introduced.

Related Commands

device-profile auto-unp-assignment	Enables auto assignment of UNP profile when the device gets identified and categorized into existing device types.
show device-profile catalog	Displays the details of known and unknown devices identified in the network.
device-profile update-signature	Updates the custom or user-defined device type to the flash and signature database.
device-profile update-signature from	Apply the new signature file in the system.

MIB Objects

```
alaDpDeviceTable
   alaDpDeviceType
   alaDpDeviceName
   alaDpDeviceMacAddress
   alaDpDeviceDhcpOpt55
   alaDpDeviceRowStatus
```

device-profile update-signature

Updates the custom or user-defined device type to the flash and signature database.

device-profile update-signature

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If the flash or the signature database is not updated with the new device type, it will not be persistent.

Example

```
-> device-profile update-signature
```

Release History

Release 8.5R2; command was introduced.

Related Commands

show device-profile catalog	Displays the details of known and unknown devices identified in the network.
device-profile update-signature from	Apply the new signature file in the system.
show device-profile signatures	Displays the device types in the local database and indicates the signatures which are not saved to the flash.

MIB Objects

```
alaDpUpdateSignature
   alaDpUpdateSignature
```

device-profile update-signature from

Applys the new signature file in the system.

device-profile update-signature from *file-name*

Syntax Definitions

file_name	The name of the file which contains device signatures.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to update the signature file in the system. Currently, only DHCP option 55 based signature is updated.
- The command also updates the custom signature into the flash.
- To view the content of the signature file, use the **show-device-profile** CLI command.

Example

```
-> device-profile update-signature from /flash/dhcp_option55_list.txt
```

Release History

Release 8.5R2; command was introduced.

Related Commands

show device-profile catalog	Displays the details of known and unknown devices identified in the network.
show device-profile signatures	Displays the device types in the local database and indicates the signatures which are not saved to the flash.
show device-profile signatures from	Displays the contents of the signature file.

MIB Objects

```
alaDpGlobalConfig
   alaDpUpdateSignatureFileName
```

device-profile auto-unp-assignment

Configures the status of automatic assignment to a UNP profile when the device gets identified and categorized into existing device types.

device-profile auto-unp-assignment

no device-profile auto-unp-assignment

Syntax Definitions

N/A

Defaults

By default, automatic assignment to a UNP profile is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the device profile is from a different VLAN, then it must be port bounced using the **unp redirect port-bounce** command to toggle.
- Use the **no** form of the command to disable the auto assignment of the UNP profile.
- When Device Profiling is globally enabled for the switch, the following UNP profiles and extended classification rules are automatically created on the switch:
  - devProfPrinter
  - devProfWindows
  - devProfIP-Phone
  - devProfWireless-Router
  - devProfSmartPhone/PDA/Tablets
- Automatically created UNP profiles are not mapped to a VLAN; manually configuring the VLAN assignment for the profile is still required.
- UNP profiles automatically created for the device types still require mapping the profiles to a VLAN.

Example

```
-> device-profile auto-unp-assignment
-> no device profile auto-unp-assignment
```

Release History

Release 8.5R2; command was introduced.

Related Commands

device-profile device-type	Adds or removes new device type and category in Device Profile.
show unp user	Displays information about the MAC addresses learned on a UNP port or link aggregate.
show unp profile	Displays the UNP profile configuration for the switch.
show unp classification-rule	Displays the UNP extended classification rule configuration for the switch.
show device-profile summary	Displays the number of devices identified based on the device type.

MIB Objects

```
alaDpGlobalConfig
   alaDpAutoUnpAssignment
```

show device-profile config

Displays the global configuration for Device Profiling.

show device-profile config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The command displays the non-default status per physical port and linkagg.
- The UNP profile auto-assignment status is also displayed.

Examples

```
-> show device-profile config

Admin-State:  Enable
UNP Auto-Assignment: Disable
Interface    Admin-Status
------------+-------------
1/1/1         Disable
1/1/2         Disable
1/1/4         Disable
0/1           Disable
```

output definitions

Admin-State	Displays the administrative status of Device Profiling.
UNP Auto-Assignment	Displays the status of automatic UNP profile assignment for the identified devices**.**
Interface	Displays the interface on which Device Profiling is configured.
Admin-Status	Displays the administrative status of Device Profiling on the interface.

Release History

Release 8.5R2; command was introduced.

Related Commands

device-profile admin-state	Enables or disables the Device Profiling configuration on the switch.
device-profile port linkagg	Enables or disables Device Profiling on the ports or linkagg interface.

MIB Objects

```
alaDpGlobalConfig
   alaDpAdminState
   alaDpAutoUnpAssignment
   alaDpDeviceRowStatus
```

show device-profile summary

Displays the number of devices identified based on the device type. Also displays information about the number of devices identified in the last one hour and one day.

show device-profile summary

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show device-profile summary

Device-Type                Total      1 Hr      1 Day
                           Count      Count     Count
-------------------------+----------+----------+------------
SmartPhone/PDA/Tablets     10         2         4
Windows                     5         0         2
IP-Camera                   2         0         2
IP-Phone                    3         3         3
Access-Points               1         1         1
Printers                    1         1         1
```

output definitions

Device-Type	Displays the name of the device type.
Total Count	Displays the total number of devices identified for the device type**.**
1 Hr Count	Displays the number of device identified in the last one hour for the device type.
1 Day Count	Displays the number of device identified in the last one day for the device type.

Release History

Release 8.5R2; command was introduced.

Related Commands

device-profile device-type	Adds or removes new device type and category in Device Profile.

MIB Objects

```
alaDpDeviceType
   alaDpDeviceRowStatus
```

show device-profile catalog

Displays the details of known and unknown devices identified in the network.

show device-profile catalog [unknown]

Syntax Definitions

unknown	Displays only the unknown devices discovered.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the option **unknown** in the CLI to display the unknown devices.

Examples

```
-> show device-profile catalog
Legend: * indicates 'Unknown/Un-catalogued' devices

Port/LAGG Device Type  Device Name Mac-Address       IP Address TimeStamp Initial  TimeStamp Most-Recent
---------+------------+-----------+-----------------+----------+------------------+---------------------
1/1/1     Smartphone    Apple      01:22:13:0E:44:42 50.50.50.3 2018-03-10 8:30:00  2018-03-12 10:30:00
1/1/2     Printers      Kyocera    00:21:23:0F:21:22 60.60.60.3 2018-03-10 8:30:00  2018-03-12 10:30:00
*1/1/3    -             -          11:32:54:0C:32:54 60.60.60.4 2018-03-10 10:00:00 2018-03-12 10:00:00
1/1/4     Access-Points Stellar    14:44:56:0A:44:23 50.50.50.6 2018-03-10 8:00:00  2018-03-12 12:30:00
2/1/10    IP Camera     Samsung    05:44:23:0D:45:66 50.50.50.3 2018-03-10 4:00:00  2018-03-12 11:30:00
```

output definitions

Port/ LAGG	Displays the port number or the linkagg ID on which the device is identified.
Device Type	Displays the device type identified**.**
Device Name	Displays the name of the device type.
MAC-Address	Displays the MAC address of the device.
IP-Address	Displays the IP address of the device.
TimeStamp Initial	Displays the time stamp when the device was first identified.
TimeStamp Most-Recent	Displays the time stamp when the device was recently active.

```
-> show device-profile catalog unknown

Port/LAGG  Mac-Address      DHCP VCI (Option 60) DHCP Option 55                    Mac-Vendor
---------+-----------------+--------------------+-----------------------------------+----------
1/1/15    34:E7:0B:03:C5:B0 HAP.1-OAW-AP1221-US 1,3,6,12,15,28,42,43,66,67,138,212 HANNetwork
1/1/13    34:E7:0B:03:C5:B1 HAP.1-OAW-AP1220-US 1,3,6,12,15,28,42,43,66,67,138,212 HANNetwork
1/1/3     11:32:54:0A:32:54 alcatel.noe.0       1,3,28,43,58,59
0/1       16:56:34:0B:33:21   -                 1,3,6,15,119,252
```

output definitions

Port/ LAGG	Displays the port number or the linkagg ID on which the device is identified.
MAC-Address	Displays the MAC address of the device.
DHCP VCI (Option 60)	Displays the DHCP option 60 information of the device.
DHCP Option 55	Displays the DHCP option 55 information of the device.
Mac-Vendor	Displays the unique MAC identifier for the vendor.

Release History

Release 8.5R2; command was introduced.
Release 8.6R1; “IP Address” field added.

Related Commands

device-profile port linkagg	Enables or disables the Device Profiling on the ports or linkagg interface.

MIB Objects

```
alaDpDeviceTable
   alaDpDeviceType
   alaDpDeviceName
   alaDpDeviceMacAddress
```

show device-profile signatures from

Displays the contents of the signature file.

show device-profile signatures from *file-name*

Syntax Definitions

file_name	The name of the file which contains device signatures.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show device-profile signatures from device_profile_sigs.csv

Device Type          Device Name                 DHCP Option 55
-------------------+-------------------+---------------------------------------
ale-ip-phone         ale-ip-phone         1,3,6,12,15,28,42,43,66,67,138,212
IP-Phone             IP-Phone             1,3,6,12,15,28,42,43,60,61,66
AP                   AP                   1,3,6,12,15,28,42,43,66,67,138,212
SmartPhone/PDA       SmartPhone           1,33,3,6,15,28,51,58,59
PDA/Tablets          PDA                  1,33,3,6,15,28,51,58,59,43
AP                   AP                   1,3,6,12,15,28,42,43,66,67,138
PDA/Tablets          Tablets              1,3,6,15,26,28,51,58,59,43

--------------------------------
Number of Signatures: 7
```

output definitions

Device Type	Displays the type of device identified.
Device Name	Displays the name of the identified device.
DHCP Option 55	Displays the DHCP Option 55 information of the identified device.

Release History

Release 8.5R2; command was introduced.

Related Commands

device-profile update-signature from	Applys the new signature file in the system.

MIB Objects

```
alaDpUpdateSignature
   alaDpUpdateSignatureFileName
```

show device-profile signatures

Displays the device types in the local database and indicates the signatures which are not saved to the flash.

show device-profile signatures

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Displays all the device types in the local database (/flash file).
- An asterisk (*) next to the device type indicates that the device signature is not saved to the flash.

Examples

```
-> show device-profile signatures

Device Type                     Device Name                    DHCP Option 55
---------------------+-------------------------+-----------------------------------------------
Wireless-Router        D-Link DI-624+            1,3,6,15
SmartPhone/PDA/Tablets Apple iPad                1,3,6,15,119,252
IP-Phone               Gigaset A580 VoIP         1,3,6,120,125,114
Printer                Kyocera Network Printer   1,3,12,23,6,15,44,47
SmartPhone/PDA/Tablets Motorola                  1,121,33,3,6,28,51,58,59
Windows                Windows XP                1,15,3,6,44,46,47,31,33,249,43
Windows_XP             MY_PC                     1,15,3,6,44,46,47,31,33,121,249,43
WIN                    new_pc                    1,15,3,6,44,46,47,31,33,121,249,252,43
NEW_WIN                this_pc                   1,15,3,6,44,46,47,31,33,121,249,43,252
Printer                SAMSUNG Network           1,3,6,7,12,15,18,23,26,44,46,51,54,58,59,78,79,81
*new                   new_name                  1,3,12,23,6,58,249

---------------------------------
Number of Signatures: 13
```

output definitions

Device Type	Displays the device type of the signature. An asterisk (*) indicates the signature of the device is not saved to the flash.
Device Name	Displays the device name associated with the device type.
DHCP Option 55	Displays the DHCP option 55 parameters associated with the device.
Number of Signatures	Displays the total number of signatures on the switch.

Release History

Release 8.5R2; command was introduced.

Related Commands

device-profile update-signature	Updates the custom or user-defined device type to the flash and signature database.

MIB Objects

```
alaDpUpdateSignature
```

40 Application Monitoring and Enforcement Commands

Application usage patterns in the enterprise network is changing with the increase in use of the social networking, browser based file sharing, and peer to peer applications. The use of these applications result in the new traffic patterns in the network that are not straightforward to distinguish. There is also an increase in consumerization of IT with multiplication of thin clients, HTTP based, and virtual desktop clients.

OmniSwitch Application Monitoring and Enforcement (AppMon) feature addresses the key challenges of real time classification of flows at application level by providing differential QoS treatment in the form of higher priority marking and security policies at application level. AppMon feature improves the quality of user experience through application aware network optimization and control.

MIB information for the AppMon commands is as follows:

Filename: ALCATEL-IND1-APP-MON-MIB.mib
Module: alaAppMonMIB

A summary of the available commands is listed here:

app-mon admin-state

Enable or disable the Application Monitoring and Enforcement (AppMon) feature.

app-mon admin-state {enable | disable}

Syntax Definitions

enable	Enables AppMon support on the switch.
disable	Disables AppMon support on the switch.

Defaults

By default, AppMon is disabled on the switch.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- AppMon cannot be enabled globally when,
  - all the mirroring sessions are used by port mirroring or monitoring features.
  - mirroring session is used by policy manager.
- When AppMon is enabled globally, it reserves a mirroring session in the system.
- If AppMon functionality is enabled at a port level, disabling AppMon globally overrides the functionality of all AppMon ports; however, configuration on the ports remain the same.
- AppMon is supported in a virtual chassis of OmniSwitch 6860 and OmniSwitch 6860E platforms where at least one OmniSwitch 6860E is mandatory for the feature to work.

Examples

```
-> app-mon admin-state enable
-> app-mon admin-state disable
```

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon port admin-state	Enable or disable AppMon on one or more switch ports.
show app-mon config	Displays global AppMon configuration, which includes information about admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

```
alaAppMonAdminStatus
```

app-mon port admin-state

Enable or disable AppMon Monitoring and Enforcement on one or more switch ports.

app-mon {port *chassis/slot/port***[**-*port2***] | slot** *chassis/slot* **[**-*slot***]} admin-state {enable | disable}**

Syntax Definitions

*chassis/slot/port***[**-*port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
chassis/slot	The chassis ID and slot number (3/1) for a specific slot.
enable	Enables AppMon on the port.
disable	Disables AppMon on the port.

Defaults

By default, AppMon is disabled on all ports.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- It is mandatory to enable AppMon globally for the port level AppMon to function.
- When slot option is used, then AppMon configuration is applied on all the physical ports of that particular slot.
- AppMon configuration is not allowed on Virtual Fabric Link, ERP, VLAN stacking, or SPB ports.
- AppMon cannot be configured on a port that is part of a link aggregate or a port mirroring port.
- AppMon must not be configured on user ports and uplink ports at the same time.

Examples

```
-> app-mon slot 1/1 admin-state enable
-> app-mon port 1/1/2-5 admin-state enable
-> app-mon slot 1/1 admin-state disable
```

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon admin-state	Enable or disable the Application Monitoring feature.
show app-mon port	Displays AppMon status per physical port or per slot for the switch.

MIB Objects

```
alaAppMonPortConfigTable
   alaAppMonPortConfigSlotPortIndex
   alaAppMonPortConfigPortStatus
```

app-mon auto-group create

Creates application groups automatically on the switch. The application groups are automatically created based on the ‘category' field of each application present in the application pool.

app-mon auto-group create

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- Modifications are allowed in auto application groups with addition or deletion of applications using the **app-mon app-group** command.
- Enter **app-mon apply** and **write memory** to save the auto group configuration or modification on the switch.
- The **show app-mon app-pool** command displays the application categories in the signature file. The application group names are derived from the category name.

Examples

```
-> app-mon auto-group create
```

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon apply	Updates the set of application signatures configured for application monitoring.
show app-mon app-group	Displays the details of all the applications in an application group.
show app-mon app-pool	Displays all the applications that are part of an application pool.

MIB Objects

```
alaAppMonAutoGroupCreation
```

app-mon app-group

Creates an application group. Applications can be added or removed from the application group.

app-mon app-group *app_group_name* **{add | remove} {app-name** *app_name* **| from** *app_name* **to** *app_name***}**

no app-mon app-group *app_group_name*

Syntax Definitions

app_group_name	Name of the application group. The group name can be a maximum of 32 alphanumeric characters.
app_name	The name of the application to be added to the application group. The application name can be a maximum of 32 alphanumeric characters.
from *app_name*	The first application name when adding a range of applications to an application group.
to *app_name*	The last application name when adding a range of applications to an application group.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- Use the **no** form of this command to remove an application group.
- This command can be used to add or delete applications for the auto application groups as well.
- One application can belong to more than one application group.
- Only those applications that are part of an application pool are allowed to be added to an application group.
- To add a range of applications or multiple applications to an application group, use the **from** and **to** options. Range is expanded based on the list of applications in the app-pool list (application pool). Use the **show app-mon app-pool** command to view the application names.
- If an application is removed from an application group which has only one application, then the complete application group is removed.
- If any application is added to a user group (group name same name as category name), and signature toolkit update operation or 'app-mon auto-group create' is done, then added group is not deleted. Only update happens.
- If an application group contains a single application and the group is part of an application list, then this single application cannot be removed from the application group.
- An application group cannot be deleted when it is part of an application list.

- When the last application from the application group is removed, the application group is automatically deleted.
- The list of applications (added or deleted) to an application group is displayed in **show configuration snapshot** command after **app-mon apply** command is entered. A list of applications (added or deleted) are displayed with the **show app-mon app-group** command even without using the **app-mon apply** command.

Examples

```
-> app-mon app-group apg2 add app-name whatsapp
-> app-mon app-group apg2 remove app-name whatsapp
-> no app-mon app-group apg2
```

To add a range of applications or multiple applications to an application group, use the **show app-mon app-pool** command to view the application names. For example:

```
-> show app-mon app-pool
Legend: Application-name: *= Not present in recently updated kit,
 AppId       Application-name             Revision       Category
-------+--------------------------------+-----------+----------------
968           amazon                        1.0.0         Web
244           facebook                      1.0.0         Web
182           sip                           1.0.0         Audio/Video
183           skype                         1.1.0         Instant Messaging
211           tftp                          1.0.0         File Server
503           twitter                       1.0.0         Web
597           viber                         1.0.0         Audio/Video
890           webex                         1.0.0         Audio/Video
1093          whatsapp                      1.0.0         Instant Messaging
240           youtube                       1.0.0         Web
--------------------------------
Number of Applications: 10
```

Select any two applications for the range option using the **app-mon app-group** command.

```
-> app-mon app-group apg1 add from sip to viber
```

This command adds the applications from sip to viber to the application group (sip, skype, tftp, twitter, and viber).

If an application is removed from an application group which has only one application, then the complete application group is removed. For example:

```
-> show app-mon app-group group1
AppGrp-Id   App-group                        App-name
----------+-----------------------------+---------------------------
1093         whatsapp                      Instant Messaging
```

Now, remove the application name ‘whatsapp’ from the application group. The complete application group gets removed as shown below.

```
-> app-mon app-group group1 remove app-name whatsapp
-> show app-mon app-group group1
AppGrp-Id   App-group                        App-name
----------+-----------------------------------+---------------------------
```

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon apply	Updates the set of application signatures configured for application monitoring.
show app-mon app-group	Displays the details of all the applications in an application group.
show app-mon app-list	Displays a list of applications and application groups added to an application list.
show app-mon app-pool	Displays all the applications that are part of an application pool.

MIB Objects

```
alaAppMonAppGroupTable
   alaAppMonAppGroupName
   alaAppMonAppGroupMember
   alaAppMonAppGroupStatus
   alaAppMonAppGrpFromAppName
   alaAppMonAppGrpToAppName
   alaAppMonAddAppGrpName
   alaAppMonAppGroupBuiltIn
   alaAppMonAppGroupCategoryName
   alaAppMonAppGrpId
   alaAppMonAppGroupAppStatus
```

app-mon app-list

Add or remove applications or application groups to an application list for enforcement or monitoring.

app-mon app-list {enforcement | monitor} {add | remove} {app-name *app_name* **| app-group** *app_group_name***}**

Syntax Definitions

add	Adds the specified application or application group to an application list.
remove	Removes the specified application or application group from an application list.
app_name	Name of the application to be added to the application list. This adds the specified application to the application list.
app_group_name	Name of the application group to be added to the application list. This enables the addition of multiple applications in the application group to the application list.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- The application group can be user created or generated automatically (see **app-mon app-group** and **app-mon auto-group create** command).
- Separate application list is maintained for enforcement and monitoring.
- The **show configuration snapshot** command displays the applications added or removed from the application list only after the **app-mon apply** command is used. The **app-mon apply** command saves the list of applications added or removed to the application list. The saved list of applications are displayed with the **show app-mon app-list active** command.
- QoS policy rules can be configured for a given application as well as an application group where the same application also exists. QoS matches policies based on the application-name or application-group name configured in an application list. For more information on configuring enforcement for QoS policy rules, see the "**QoS Policy Commands**" chapter.

Examples

```
-> app-mon app-list enforcement add app-name whatsapp
-> app-mon app-list enforcement add app-group apg1
-> app-mon app-list monitor add app-group apg2
-> app-mon app-list enforcement remove app-name whatsapp
```

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon auto-group create	Enables or disables Auto-Group functionality on the switch.
app-mon app-group	Creates an application group. Applications can be added or removed from the application group.
show app-mon app-list	Displays list of applications and application groups added to an application list.
clear app-mon app-list	Removes all applications signatures from the application list.

MIB Objects

```
alaAppMonAppListTable
   alaAppMonAppListMemberName
   alaAppMonAppListMemberType
   alaAppMonAppListMemberStatus
   alaAppMonAppListAppId
   alaAppMonAppListAppStatus
```

app-mon apply

This activates both enforcement and monitoring application lists for flow classification.

app-mon apply

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

The following operations are performed with the **app-mon apply** command:

- Saves the current application-list, application-group, and auto-groups to flash when 'write memory' command is used.
- The application list is checked for any application configured more than once in an application list (individually or as a part of application group).
  - The **app-mon apply** command will not be successful until the conflict is resolved.
  - The **show app-mon app-list** command with the **monitor conflict** or the **enforcement conflict** parameter displays the available conflicts in an application list.
  - The duplicate application names must be removed for a successful **app-mon apply** operation.
- QoS is applied to the flows learned for the activated applications based on the configured QoS policies for Enforcement application list.

Examples

```
-> app-mon apply
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.
show app-mon port	Displays AppMon status per physical port or per slot for the switch.
show app-mon app-list	Displays a list of applications and application groups added to an application list.

MIB Objects

```
alaAppMonUpdateAppList
```

app-mon l3-mode

Enables or disables monitoring and enforcement for IPv4 flows, IPv6 flows, or both.

app-mon l3-mode {ipv4 | ipv6} admin-state {enable | disable}

Syntax Definitions

IPv4	Applies monitoring and enforcement to IPv4 flows.
IPv6	Applies monitoring and enforcement to IPv6 flows.
enable	Enables the specified L3 mode on the switch.
disable	Disables the specified L3 mode on the switch.

Defaults

By default, monitoring and enforcement is enabled for both IPv4 and IPv6 flows.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

N/A

Examples

```
-> app-mon l3-mode ipv4 admin-state disable
-> app-mon l3-mode ipv4 admin-state enable
-> app-mon l3-mode ipv6 admin-state disable
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon ipv4-flow-table	Displays the flow table for IPv4 flows entries for enforcement and monitor flows.
show app-mon ipv6-flow-table	Displays the flow table for IPv6 flows entries for enforcement and monitor flows.
show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

```
alaAppMonEnforcementIpv4
alaAppMonEnforcementIpv6
```

app-mon l4-mode

Enables or disables monitoring and enforcement for TCP or UDP flows.

app-mon {port *chassis/slot/port***[-***port2***] | slot** *chassis/slot***} l4-mode {tcp | udp} admin-state {enable | disable}**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
chassis/slot	The chassis ID and slot number (3/1) for a specific slot.
tcp	Applies monitoring and enforcement to TCP flows.
udp	Applies monitoring and enforcement to UDP flows.
enable	Enables the specified L4 mode on the switch.
disable	Disables the specified L4 mode on the switch.

Defaults

By default, both TCP and UDP flows are processed.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

N/A

Examples

```
-> app-mon port 1/1/2 l4-mode udp admin-state disable
-> app-mon slot 1/1 l4-mode tcp admin-state enable
-> app-mon port 1/1/2 l4-mode udp admin-state enable
```

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon l4port-exclude	Configures the L4 port range to exclude from the AppMon operation.
show app-mon ipv4-flow-table	Displays the flow table for IPv4 flows entries for enforcement and monitor flows.
show app-mon ipv6-flow-table	Displays the flow table for IPv6 flows entries for enforcement and monitor flows.
show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

```
alaAppMonPortConfigTable
   alaAppMonPortConfigSlotPortIndex
   alaAppMonEnforcementPortConfigTcpStatus
   alaAppMonEnforcementPortConfigUdpStatus
```

app-mon l4port-exclude

Configures the L4 port range to exclude from the AppMon operation.

app-mon l4port-exclude range-id *number* **{tcp-service-port | udp-port} start** *number* **end** *number*

no app-mon l4port-exclude range-id

Syntax Definitions

range-id *number*	The range ID number. The valid range is 1–8.
tcp-service-port	Specifies TCP service ports.
udp-port	Specifies UDP ports.
start *number*	The first port associated with the range ID number. The valid port range is 1–65535.
end *number*	The last port associated with the range ID number. The valid port range is 1–65535.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- Use the **no** form of this command to remove an L4 exclude range ID from the switch configuration.
- For the **udp-port** option, the AppMon operation is not performed on the flows with a source or destination port that is in the excluded port range.
- For the **tcp-service-port** option, the AppMon operation is not performed on the flows with a destination TCP port of TCP-SYN packet or a source TCP port of TCP-SYN-ACK packet that is in the excluded port range.
- This configuration applies to both enforcement and monitor features.

Examples

```
-> app-mon l4port-exclude range-id 5 tcp-service-port start 20 end 30
-> app-mon l4port-exclude range-id 6 udp-port start 90 end 100
-> no app-mon l4port-exclude range-id 6
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon l4port-exclude Displays the port range excluded from AppMon operation.

MIB Objects

```
alaAppMonEnforcementL4PortRangeTable
   alaAppMonEnforcementL4PortRangeStart
   alaAppMonEnforcementL4PortRangeEnd
   alaAppMonEnforcementL4PortType
   alaAppMonEnforcementL4PortStatus
```

app-mon flow-table flush

Clears all the learned flow-table entries for both IPv4 and IPv6 flow tables.

app-mon flow-table {enforcement | monitor} flush

Syntax Definitions

enforcement	Flushes all the learned flow-table entries from the enforcement application.
monitor	Flushes all the learned flow-table entries from the monitor application.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- When the **enforcement** option is used, all the active flows information are cleared; no QoS treatment is provided (if configured). The data (active, gross counters, statistics, and flow information) in the following commands are cleared: **show app-mon app-list enforcement active**, **show app-mon app-list enforcement active stats**, **show app-mon ipv4-flow-table enforcement**, **show app-mon ipv6-flow-table enforcement**, **show app-mon stats**.
- When the **monitor** option is used, all the learned flows information will be cleared. The data (gross counters and flow information) in the following commands are cleared: **show app-mon app-list monitor active**, **show app-mon ipv4-flow-table monitor**, **show app-mon ipv6-flow-table monitor**.
- When this command is used, application-record information is not cleared.

Examples

```
-> app-mon flow-table enforcement flush
-> app-mon flow-table monitor flush
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.
show app-mon app-list	Displays a list of applications and application groups added to an application list. ‘stats’ option in this command displays active or gross packets/byte counters on per application basis.
show app-mon ipv4-flow-table	Displays the flow table for IPv4 flows entries for enforcement and monitor flows.
show app-mon ipv6-flow-table	Displays the flow table for IPv6 flows entries for enforcement and monitor flows.

MIB Objects

```
alaAppMonFlowTableFlush
```

app-mon flow-table enforcement stats

Enable or disable flow table statistics update for enforcement applications.

app-mon flow-table enforcement stats admin-state {enable | disable}

Syntax Definitions

enable	Enable flow-table statistics update.
disable	Disable flow-table statistics update.

Defaults

By default, statistics admin status is disabled.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- This command is applicable only for enforcement applications.
- The statistics collection capability is shared with Service Manager, which means that either the Service Manager feature or AppMon can use this capability at any given time. Hence, disabling the counter usage in Service Manager using the **service stats disable** command is required to view the flow table statistics update for enforcement applications. For more information about this command, see the "Service Manager Commands" chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.
- When update statistics is enabled, the updated statistics is displayed in the **show app-mon ipv4-flow-table enforcement verbose**, **show app-mon ipv6-flow-table enforcement verbose**, and **show app-mon app-list enforcement active stats** commands. Statistics are refreshed every 160 seconds from data path, and based on the flow sync interval between the data path and the control path.

Examples

```
-> app-mon flow-table enforcement stats admin-state enable
-> app-mon flow-table enforcement stats admin-state disable
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

```
alaAppMonEnforcementFlowTableStatsAdminStatus
```

app-mon aging enforcement

Configures aging time for dynamically learned TCP/UDP flows for each application for Enforcement applications.

app-mon aging enforcement app-name *app_name* **[tcp | udp] interval {120m | 60m | 30m | 10m | 5m | 3m | default}**

Syntax Definitions

app_name	Name of the application to configure its aging interval. The application must be part of the application pool.
interval	The aging time interval for dynamically learned flows in the flow table, in minutes.
default	Configures the default aging interval.

Defaults

By default, aging interval is set per application and TCP or UDP flow type basis.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- User can set separate TCP or UDP flows aging interval for an given application.
- When TCP option is used to configure aging interval for an application, TCP flows generated by a given application age out with configured value.
- When UDP option is used to configure aging interval for an application, UDP flows generated by a given application age out with configured value.
- Flow aging is supported for the applications that are part of the enforcement application list. Flows related with enforcement application list are made active for QoS treatment as well statistics collection.
- Flow aging is not supported for applications that are part of Monitor application list. Monitor flow tables log these flows when they are detected until logging threshold is reached.

Examples

```
-> app-mon aging enforcement app-name sip tcp interval 60m
-> app-mon aging enforcement app-name tftp udp interval 120m
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.
show app-mon aging enforcement	Displays the aging interval for each application for enforcement feature.

MIB Objects

```
alaAppMonEnforcementAgingTimerTable
   alaAppMonEnforcementAgingTimerValue
```

app-mon logging-threshold

Configures the threshold for the number of matched flows for enforcement and monitor applications.

app-mon logging-threshold {enforcement | monitor} num-of-flows {*number* | **default}**

Syntax Definitions

number	Threshold value for the number of matched flows. The valid range is 1000–60000.
default	Sets the threshold back to the default value of 20K.

Defaults

By default, 20000 flows are logged.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- When the logging threshold value is set to ‘0’, flows are not logged to the log file.
- When used with enforcement option, it configures the threshold for the number of matched flows to be saved on to the log file for enforcement applications.
- When used with monitor option, it configures the threshold for the number of matched flows to be displayed in the monitor flow table commands.

Examples

```
-> app-mon logging-threshold monitor num-of-flows 10000
-> app-mon logging-threshold monitor num-of-flows default
-> app-mon logging-threshold enforcement num-of-flows 10000
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information about admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

```
alaAppMonThresholdNumberOfFlows
```

app-mon flow-sync enforcement interval

Configures the interval at which the enforcement flows information is refreshed.

app-mon flow-sync enforcement interval {*number* **| default}**

Syntax Definitions

number	Flow sync interval at which the enforcement flows information is refreshed. The valid range is 10–3600 seconds. The interval can be configured only for the enforcement feature.
default	Configures the default flow-sync interval.

Defaults

Default flow-sync interval is 60 seconds for enforcement.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

The refreshed information is shown in the following show commands: **show app-mon applist enforcement active**, **show app-mon applist enforcement active stats**, **show app-mon ipv4-flow-table enforcement**, **show app-mon stats**.

Examples

```
-> app-mon flow-sync enforcement interval 10
-> app-mon flow-sync enforcement interval default
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon ipv4-flow-table	Displays the flow table for IPv4 flows entries.
show app-mon ipv6-flow-table	Displays the flow table for IPv6 flows entries.

MIB Objects

```
alaAppMonFlowSyncEnforcementInterval
```

app-mon force-flow-sync

Synchronizes flows learned in the data path.

app-mon force-flow-sync {enforcement | monitor}

Syntax Definitions

enforcement	Synchronizes flows learned in the data path for the enforcement feature from the hardware.
monitor	Synchronizes flows learned in the data path for the monitor feature from the hardware.

Defaults

By default, flow synchronization occurs every 5 minutes for monitor flows and 60 seconds for enforcement flows.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

Use this command to force a flow synchronization with the control path database in real time.

Examples

```
-> app-mon force-flow-sync enforcement
-> app-mon force-flow-sync monitor
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon ipv4-flow-table	Displays the flow table for IPv4 flows entries.
show app-mon ipv6-flow-table	Displays the flow table for IPv6 flows entries.

MIB Objects

```
alaAppMonForceFlowSyncStatus
```

show app-mon config

Displays global AppMon configuration, which includes information about admin-state, running mode, IP mode, aging-timer, and total signatures.

show app-mon config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

The operational state is enabled if there is at least one OmniSwitch 6860E chassis in the virtual chassis (VC). If there is no OmniSwitch 6860E in the VC, the operational-state is disabled.

Examples

```
-> show app-mon config
Admin State                          : Enable,
Operational State                    : Enable,
L3-IPv4                              : Enable,
L3-IPv6                              : Enable,
Enforcement Flow-Table Stats         : Enable,
Enforcement Flow-Sync Interval       : 10 seconds,
Monitor Logging Threshold            : 20000,
Enforcement Logging Threshold        : 20000,
App-Pool Applications                : 10,
Monitor Applied Applications         : 10,
Enforcement Applied Applications     : 10,
Upgraded Signature File Type         : Factory,
AOS Compatible Signature Kit Version : 1,
Signature Kit version                : 1.1.1
```

output definitions

Admin-state	The AppMon administrative status (**Enabled** or **Disabled**). Configured through the **app-mon admin-state** command.
Operational State	The operational status (**Enabled** or **Disabled**).
L3-IPv4	Status of IPv4 l3 mode on the switch (**Enable** or **Disable**)
L3-IPv6	Status of IPv6 l3 mode on the switch (**Enable** or **Disable**)
Enforcement Flow-Table Stats	Status of the enforcement flow table statistics update.
Enforcement Flow Sync interval	Enforcement flow sync interval at which the switch polls for flow information.

output definitions (continued)

Monitor Logging-Threshold	Monitor threshold value for the flows to be saved in the IPv4 or IPv6 flow table.
Enforcement Logging-Threshold	Enforcement threshold value for the flows to be saved on to the log file.
App-Pool Applications	The number of application signatures in the application pool.
Monitor Applied Applications	The number of active applications in the Monitor application list.
Enforcement Applied Applications	The number of active applications in the enforcement application list.
Upgraded Signature File Type	The signature file type: Factory or Production
AOS Compatible Signature Kit Version	Determines the compatibility between AOS software and the signature file.
Signature Kit version	The signature file version that contains the application signatures.

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon port	Displays AppMon status per physical port or per slot.

MIB Objects

```
alaAppMonAdminStatus
alaAppMonOperStatus
alaAppMonAgingInterval
alaAppMonAppliedApplications
alaAppMonAppPoolApplications
alaAppMonSignatureFileVersion
alaAppMonLoggingThreshold
alaAppMonKitCompatabilityVersion
alaAppMonAOSCompatabilityVersion
alaAppMonAutoGroupCreation
```

show app-mon port

Displays AppMon status per physical port or per slot for the switch.

show app-mon [port *chassis/slot/port* **| slot** *chassis/slot***]**

Syntax Definitions

*chassis/slot/port***[-***port2***]**	The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
chassis/slot	The chassis ID and slot number (3/1) for a specific slot.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

N/A

Examples

```
-> show app-mon port
  Port     Admin-Status   Oper-Status       L4-mode
----------+-------------+-----------------+---------------
1/1/1       Enable         Up                TCP-UDP
1/1/2       Enable         Up                TCP-UDP
1/1/3       Enable         Up                TCP-UDP
1/1/4       Enable         Up                TCP-UDP
1/1/5       Enable         Up                TCP-UDP
1/1/6       Enable         Up                TCP-UDP
1/1/7       Enable         Up                TCP-UDP
.
.
.

-> show app-mon slot 1/1
  Port     Admin-Status   Oper-Status       L4-mode
----------+-------------+-----------------+---------------
1/1/1       Enable         Up                TCP-UDP
1/1/2       Enable         Up                TCP-UDP
1/1/3       Enable         Up                TCP-UDP
1/1/4       Enable         Up                TCP-UDP
1/1/5       Enable         Up                TCP-UDP
1/1/6       Enable         Up                TCP-UDP
1/1/7       Enable         Up                TCP-UDP
1/1/8       Enable         Up                TCP-UDP
.
.
.
```

output definitions

Port	The chassis identifier, slot, and port on which AppMon is enabled or disabled.
Admin-Status	Indicates the admin status of the port.
Oper-Status	Indicates the operational status of the port.
L4-mode	Indicates the L4 mode: TCP or UDP.

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

```
alaAppMonPortConfigTable
   alaAppMonPortConfigSlotPortIndex
   alaAppMonPortConfigPortStatus
   alaAppMonPortConfigPortOperStatus
   alaAppMonPortConfigPortType
```

show app-mon app-pool

Displays all the applications that are part of an application pool.

show app-mon app-pool

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

N/A

Examples

```
-> show app-mon app-pool
Legend: Application-name: *= Not present in recently updated kit,
 AppId       Application-name             Revision       Category
-------+--------------------------------+------------+----------------
968           amazon                        1.0.0         Web
244           facebook                      1.0.0         Web
182           sip                           1.0.0         Audio/Video
183           skype                         1.1.0         Instant Messaging
211           tftp                          1.0.0         File Server
503           twitter                       1.0.0         Web
597           viber                         1.0.0         Audio/Video
890           webex                         1.0.0         Audio/Video
1093          whatsapp                      1.0.0         Instant Messaging
240           youtube                       1.0.0         Web

---------------------------------
Number of Applications: 10
```

output definitions

AppId	Identity of the application group.
Application-name	Name of the application group whose details are viewed. **Note: * indicates that the application is not present in the recently updated signature file.**
Revision	Application revision number.
Category	Application category name.

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

```
alaAppMonAppPoolTable
   alaAppMonAppPoolAppName
   alaAppMonAppPoolCategory
   alaAppMonAppPoolRevision
   alaAppMonAppPoolAppStatus
```

show app-mon app-list

Displays a list of applications and application groups added to an application list.

show app-mon app-list {monitor | enforcement} [active [stats]] [conflict]

Syntax Definitions

monitor	Displays information for applications added for monitoring.
enforcement	Displays information for applications added for enforcement.
active [stats]	Displays the list of activated applications in an application list. Use the **stats** option together with the **enforcement** option.
conflict	Displays the list of applications that are present more than once in an application list.

Defaults

By default, all applications and application groups that belong to an application list are displayed.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- Use the **conflict** option to identify applications that are present more than once in an application list. This needs to be checked and resolved for **app-mon apply** to be successful.
- The **active** option displays active and gross number of flows detected on per application basis.
- For monitor feature, **active** option displays only the gross counters.
- The **stats** option is used only for the **enforcement** option. This displays active or gross packets/byte counters per application basis.

Examples

```
-> show app-mon app-list monitor
App-Id/        Application-List                          Application-List
AppGrp-Id      Member Name                               Member Type
------------+-----------------------------------------+---------------------
244            facebook                                   APP
182            sip                                        APP-GRP
```

output definitions

App-Id/AppGrp-Id	Identity of the application or application group.
Application-List Member Name	Name of the application group or application.
Application-List Member Type	Specifies the application type: individual application or whether the application belongs to any application group.

```
-> show app-mon app-list monitor active
Legend: Application-name: *= Not present in recently updated kit,

App-Id     Application            App-Grp               Matched
           Name                   Name                  Gross Count
-------+--------------------+-----------------------+-----------------
968        amazon                 APP                    0
244        facebook               APP                    0
211        tftp                   APP-GRP                24508
Number of Applications: 3
```

output definitions

App-ID	Identity of the application group.
Application Name	Name of the application.
App-Grp Name	Name of the application group.
Matched Gross Count	Total number of matched active flows per application.
Number of Applications	Total number of active applications in the application list.

```
-> show app-mon app-list monitor conflict
Sn   App-ID     Application-Name        Application-Group     Error-Type
----+-------+-----------------------+--------------------+---------------
1     244        facebook                  APP               Duplicate
2     244        facebook                  APP               Duplicate
```

output definitions

Sn	The serial number.
App-ID	Identity of the application group.
Application-Name	Name of the application.
Application-Group	Name of the application group.
Error-Type	Displays the type of error.

```
-> show app-mon app-list enforcement
Legend: Application-name: *= Not present in recently updated kit,
App-Id/        Application-List                  Application-List
AppGrp-Id      Member Name                       Member Type
------------+-----------------------------------+--------------------------
244             facebook                              grp1
```

output definitions

App-Id/AppGrp-Id	Identity of the application or application group
Application-List Member Name	Name of the application group or application. **Note: * indicates that the application is not present in the recently updated signature file.**
Application-List Member Type	Specifies the application type: individual application or whether the application belongs to any application group.

```
-> show app-mon app-list enforcement active
Legend: Application-name: *= Not present in recently updated kit,
App-Id   Application              App-Grp              Matched     Matched
         Name                     Name                 Flow Count  Gross Count
------+---------------------+----------------------+-----------+------------
968       amazon                  grp1                  0              0
182       sip                     grp1                  0              0
211       tftp                    grp1                  0              0
890       webex                   grp2                  0              0
1093      whatsapp                grp2                  0              0
183       skype                   grp1                  0              0
597       viber                   grp2                  0              0
244       facebook                grp1                 7837           8192
503       twitter                 grp1                  0              0
240       youtube                 grp2                  0              0
Number of Applications: 10
```

output definitions

Application Name	Name of the application. **Note: * indicates that the application is not present in the recently updated signature file.**
App-Id	Identity of the application group.
App-Group Name	Name of the application group.
Matched Flow Count	Number of matched active flows per application.
Matched Gross Count	Total number of matched flows per application.
Number of Applications	Total number of active applications in the application list.

```
-> show app-mon app-list enforcement active stats
Legend: Application-name: *= Not present in recently updated kit,

App-Id Application App-Grp  Matched Active Matched Active  Matched Gross  Matched Gross
        Name       Name     Packet Count   Byte Count      Packet Count   Byte Count
------+----------+--------+--------------+-------------+-------------+--------------
182      SIP        grp1         1236          15236           1000        15000
211      TFTP       grp1         2000          345678          3456        604569
```

output definitions

Application Name	Name of the application. **Note: * indicates that the application is not present in the recently updated signature file.**
App-Id	Identity of the application group.
App-Group Name	Name of the application group.
Matched Active Packet Count	Packet count of active matched flows.
Matched Active Byte Count	Byte count of active matched flows
Matched Gross Packet Count	Cumulative packet count of active matched flows and ended flows.
Matched Gross Byte Count	Cumulative byte count of active matched flows and ended flows.

```
-> show app-mon app-list enforcement conflict

Sn   App-ID     Application-Name        Application-Group     Error-Type
----+-------+-----------------------+--------------------+---------------
1      244       facebook                grp1               Duplicate
2      244       facebook                grp1               Duplicate
```

output definitions

Sn	The serial number.
App-ID	Identity of the application group.
Application-Name	Name of the application.
Application-Group	Name of the application group.
Error-Type	Displays the type of error.

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.
show app-mon app-group	Displays the details of all the applications in an application group.

MIB Objects

alaAppMonActiveAppListTable

- alaAppMonAppListMemberName
- alaAppMonAppListMemberType
- alaAppMonAppListMemberStatus
- alaAppMonAppListAppId
- alaAppMonAppListAppStatus

alaAppMonActiveAppListTable

- alaAppMonActiveAppListAppName
- alaAppMonActiveAppListAppGroupName
- alaAppMonActiveAppListAppId
- alaAppMonActiveAppListAppStatus

alaAppMonAppListConflictTable

- alaAppMonAppListConflictIndex
- alaAppMonAppListConflictAppName
- alaAppMonAppListConflictAppId
- alaAppMonAppListConflictAppGroupName
- alaAppMonAppListConflictErrorType

alaAppMonEnforcementAppListTable

- alaAppMonEnforcementAppListMemberName
- alaAppMonEnforcementAppListAppOrGroupID
- alaAppMonEnforcementAppListMemberType
- alaAppMonEnforcementAppListAppStatus
- alaAppMonEnforcementAppListMemberStatus

alaAppMonEnforcementActiveAppListTable

- alaAppMonEnforcementActiveAppListAppName
- alaAppMonEnforcementActiveAppListAppGroupName
- alaAppMonEnforcementActiveAppListActiveMatchedFlows
- alaAppMonEnforcementActiveAppListTotalMatchedFlows
- alaAppMonEnforcementActiveAppListAppID
- alaAppMonEnforcementActiveAppListAppStatus
- alaAppMonEnforcementActiveAppListActivePktCount
- alaAppMonEnforcementActiveAppListActiveByteCount
- alaAppMonEnforcementActiveAppListGrossPktCount
- alaAppMonEnforcementActiveAppListGrossByteCount

alaAppMonEnforcementAppListConflictTable

- alaAppMonEnforcementAppListConflictIndex
- alaAppMonEnforcementAppListConflictAppID
- alaAppMonEnforcementAppListConflictAppName
- alaAppMonEnforcementAppListConflictAppGrpName
- alaAppMonEnforcementAppListConflictAppErrorType

show app-mon app-group

Displays the details of all the applications in an application group.

show app-mon app-group [group-name *group_name***]**

Syntax Definitions

group_name	The name of an application group. This is a case sensitive string.

Defaults

By default, information is displayed for all application groups.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

- This command displays both user created and automatically created application groups and the applications added to the respective group.
- Application names which are added to group and not yet activated are also displayed.
- This also display the auto application groups.

Examples

```
-> show app-mon app-group
Legend: Application-name: *= Not present in recently updated kit,

AppGrp-Id  App-group                              App-name
----------+--------------------------------------+-------------------------
AG-1       Web                                    amazon
                                                  facebook
                                                  twitter
                                                  youtube
AG-2       Instant Messaging                      whatsapp
                                                  skype
AG-3       Audio/Video                            sip
                                                  viber
                                                  webex
AG-4       File Server                            tftp
```

output definitions

AppGrp-Id	Identity of the application group.
App-group	Name of the application group whose details are viewed.
App-name	Name of the applications attached to the application group.

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.
show app-mon app-list	Displays list of applications and application groups added to an application list.

MIB Objects

```
alaAppMonAppGroupTable
   alaAppMonAppGroupName
   alaAppMonAppGroupMember
   alaAppMonAppGroupCategoryName
   alaAppMonAppGrpId
   alaAppMonAppGroupAppStatus
   alaAppMonAppGroupStatus
```

show app-mon app-record

Displays current-hour application-record information as well the historic application-records on the hourly or 24-hours basis for monitored applications.

show app-mon app-record [hourly | twenty-four-hours | current-hour] [verbose]

Syntax Definitions

hourly	Displays flows detected for an applications in an hour. An Hour is defined with fixed boundary (for example, 1:30 p.m to 2:30 p.m).
twenty-four-hours	Displays aggregate of available 'hourly' records for each application, flows detected in last 24-hours since last hour boundary. 'current-hour' data will not be part of this. This information is updated every one hour when 'hourly' record is updated.
current-hour	Displays new flow detected for an application in the current hour which is not part of 'hourly' historic data. When current-hour reaches an hour boundary, this data is moved to 'hourly' records. For example, if current time is 2.40 p.m, then information between 2.30 p.m to 2.40 p.m is displayed. On 3.30 p.m, current-hour information is moved to the latest hourly record.
verbose	Select this option to view detail information for each option. Detail information include minimum, maximum and average flows detected for each application.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This is supported for monitoring.

Examples

```
-> show app-mon app-record current-hour
Sampling Interval Every 5-minutes
 Application                        Application group         Total Detected Flows
---------------------------------+--------------------------+---------------------
2015-07-28 15:30:00 IST 0d 00h 48m 11s
sip                                  grp1                           11
youtube                              grp1                           16572
--------------------------------
Number of Applications: 2
```

```
-> show app-mon app-record hourly
Sampling Interval Every 5-minutes
Application                  Application group         Total Detected Flows
-----------------------+----------------------------+-----------------------
2015-07-28 13:30:00 IST 0d 01h 00m 00s
youtube                          grp1                            21534
--------------------------------
--------------------------------
Number of Applications: 2
--------------------------------+-------------------------------------------------
2015-07-28 14:30:00 IST 0d 01h 00m 00s
facebook                         grp2                            24

--------------------------------
--------------------------------
Number of Applications: 1
--------------------------------+-------------------------------------------------
Number of hourly App-Records: 2

-> show app-mon app-record hourly verbose
Sampling Interval Every 5-minutes
Application    Application group                  Detected Flows
                                        Min.        Max.         Avg.        Total
-------------+--------------------+-----------+-----------+-----------+------------
2015-07-28 13:30:00 IST 0d 01h 00m 00s
facebook             grp2              1           2           1         7
youtube              grp1              1184        12600       7178      21534

--------------------------------
--------------------------------
Number of Applications: 2
--------------------------------+-------------------------------------------------
2015-07-28 14:30:00 IST 0d 01h 00m 00s
facebook             grp2               1           1                1
4
--------------------------------
--------------------------------
Number of Applications: 1
--------------------------------+-------------------------------------------------
Number of hourly App-Records: 2

-> show app-mon app-record twenty-four-hours
Sampling Interval Every 5-minutes
2015-10-09 12:30:00 IST 1d 00h 00m 00s

Application                        Total Detected Flows (24-hours)
-----------------------------+-----------------------------------------
skype                                471
youtube                              4239
facebook                             102
twitter                              2
viber                                99
whatsapp                             13
--------------------------------
Number of Applications: 6
```

```
-> show app-mon app-record twenty-four-hours verbose
Sampling Interval Every 5-minutes
2015-10-09 12:30:00 IST 1d 00h 00m 00s

Application                          Detected Flows (24-hours)
                                Min.          Max.          Avg.         Total
----------------------------+-------------+-------------+-------------+----------
skype                            2             111           52           471
youtube                          1             1200          529          4239
facebook                         4             15            7            102
twitter                          2             2             2            2
viber                            1             35            9            99
whatsapp                         1             4             1            13
--------------------------------
Number of Applications: 6
```

output definitions

Application	Name of the application.
Application group	Name of the application group.
Detected Flows	**Min**: Minimum number of flows that were detected. **Max**: Maximum number of flows that were detected. **Avg**: Average number of flows that were detected. **Total**: Total number of flows that were detected
Number of Applications	Displays the total number of applications.

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays the global AppMon configuration.

MIB Objects

```
alaAppMonAppRecCurrentHrStatsTable
   alaAppMonAppRecCurrentHrStatsName
   alaAppMonAppRecCurrentHrStatsMinActiveFlow
   alaAppMonAppRecCurrentHrStatsMaxActiveFlow
   alaAppMonAppRecCurrentHrStatsAvgActiveFlow
   alaAppMonAppRecCurrentHrStatsTotalFlow
alaAppMonAppRecHrlyStatsTable
   alaAppMonAppRecHrlyStatsName
   alaAppMonAppRecHrlyStatsMinActiveFlow
   alaAppMonAppRecHrlyStatsMaxActiveFlow
   alaAppMonAppRecHrlyStatsAvgActiveFlow
   alaAppMonAppRecHrlyStatsTotalFlow
alaAppMonAppRec24HrStatsTable
   alaAppMonAppRec24HrStatsName
   alaAppMonAppRec24HrStatsMinActiveFlow
   alaAppMonAppRec24HrStatsMaxActiveFlow
   alaAppMonAppRec24HrStatsAvgActiveFlow
   alaAppMonAppRec24HrStatsTotalFlow
```

show app-mon ipv4-flow-table

Displays the flow table for IPv4 flows entries for enforcement and monitor flows.

show app-mon ipv4-flow-table {monitor | enforcement [verbose]} [{src-ipv4 | dest-ipv4} *ip_address*] **[app-name** *app_name* **| app-group** *grp_name*]

Syntax Definitions

verbose	Displays detailed information of the flows.
src-ipv4 *ip_address*	Filter flow table based on the specified source IPv4 address.
dest-ipv4 *ip_address*	Filter flow table based on the specified destination IPv4 address.
app_name	Filter flow table based on application name.
grp_name	Filter flow table based on application group.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

The **verbose** option displays additional information about the flow start time, statistics counters, associated application group, policy rule, and so on. This option is supported only for enforcement feature.

Examples

```
-> show app-mon ipv4-flow-table monitor
SrcIP            DestIP       SrcPort     DestPort    Proto     App Name  App Group
-------------+-------------+----------+-----------+---------+----------+---------
100.0.0.10      101.0.0.10       48128      3128       TCP        facebook     test
100.0.0.10      101.0.0.10       48384      3128       TCP        facebook     test
100.0.0.10      101.0.0.10       48640      3128       TCP        facebook     test
100.0.0.10      101.0.0.10       48896      3128       TCP        facebook     test
.
.
.

-> show app-mon ipv4-flow-table monitor src-ipv4 103.20.92.80
SrcIP            DestIP        sPort   dPort   Proto    App Name     App-Group Name
-------------+-------------+-------+-------+------+------------+--------------
103.20.92.80   192.168.1.3      443    61069    TCP     whatsapp         test

Number of flows : 1
```

```
-> show app-mon ipv4-flow-table monitor dest-ipv4 74.112.124.120
SrcIP            DestIP         sPort   dPort   Proto    App Name     App-Group Name
-------------+---------------+-------+-------+------+-------------+--------------
209.226.67.175 74.112.124.120   2458    9673    TCP     whatsapp        test

Number of flows : 1

-> show app-mon ipv4-flow-table monitor app-name youtube
SrcIP            DestIP         sPort   dPort   Proto    App Name     App-Group Name
-------------+---------------+-------+-------+------+-------------+--------------
207.219.97.56   74.125.225.0    1410     80     TCP     youtube          test

Number of flows : 1
```

output definitions

SrcIP	Displays flow table based on the specified source IPv4 IP address.
DestIP	Displays flow table based on the specified destination IPv4 IP address.
SrcPort	Source port of the flow entry.
DestPort	Destination port of the flow entry.
Proto	Indicates the protocol type (TCP or UDP)
App Name	Displays the flow table based on the application name.
App-Group	Displays the flow table based on the application group.

```
-> show app-mon ipv4-flow-table enforcement
SrcIP             DestIP         SrcPort    DestPort    Proto      App Name
-------------+-------------+-----------+-----------+---------+---------------
100.0.0.10      101.0.0.10      48128       3128        TCP       facebook
100.0.0.10      101.0.0.10      48384       3128        TCP       facebook
100.0.0.10      101.0.0.10      48640       3128        TCP       facebook
100.0.0.10      101.0.0.10      48896       3128        TCP       facebook
100.0.0.10      101.0.0.10      49152       3128        TCP       facebook
100.0.0.10      101.0.0.10      49408       3128        TCP       facebook
100.0.0.10      101.0.0.10      49664       3128        TCP       facebook
100.0.0.10      101.0.0.10      49920       3128        TCP       facebook
.
.
.

-> show app-mon ipv4-flow-table enforcement verbose
Legend: start/date/time/zone  duration
SrcIp       DestIP   SrcPort DestPort Protocol Application-name App-group Policy rule Packet Count Byte Count,
--------------------------------------------------------------------------------
2015-07-24/15:01:34/IST     0d 0h 1m 42s
100.0.0.10 101.0.0.10 48128   3128     TCP       facebook         test     app-mon1      0           0
2015-07-24/15:01:36/IST     0d 0h 1m 40s
100.0.0.10 101.0.0.10 48384   3128     TCP       facebook         test     app-mon1      0           0
2015-07-24/15:01:38/IST     0d 0h 1m 38s
100.0.0.10 101.0.0.10 48640   3128     TCP       facebook         test     app-mon1      0           0
2015-07-24/15:01:39/IST     0d 0h 1m 37s
100.0.0.10 101.0.0.10 48896   3128     TCP       facebook         test     app-mon1      0           0
2015-07-24/15:01:41/IST     0d 0h 1m 35s
100.0.0.10 101.0.0.10 49152   3128     TCP       facebook         test     app-mon1      0           0
2015-07-24/15:01:43/IST     0d 0h 1m 33s
100.0.0.10 101.0.0.10 49408   3128     TCP       facebook         test     app-mon1      0           0
2015-07-24/15:01:45/IST     0d 0h 1m 31s.
.
.
.
```

output definitions

SrcIP	Source IPv4 address of the flow.
DestIP	Destination IPv4 address of the flow.
SrcPort	Source port of the flow entry.
DestPort	Destination port of the flow entry.
Protocol	Indicates the protocol type (TCP or UDP)
Application Name	Name of the application.
App-group	Name of the application group.
Policy rule	The QoS policy applied for enforcement.
Packet Count	Number of packet counts that match a flow table entry in the hardware.
Byte Count	Number of byte counts that match a flow table entry in the hardware.

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays global AppMon configuration, which includes information like admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

```
alaAppMonFlowTable
   alaAppMonFlowSourceIPType
   alaAppMonFlowSourceIP
   alaAppMonFlowDestIPType
   alaAppMonFlowDestIP
   alaAppMonFlowSrcPort
   alaAppMonFlowDestPort
   alaAppMonFlowProtocol
   alaAppMonFlowAppName
alaAppMonEnforcementFlowTable
   alaAppMonEnforcementFlowSourceIPType
   alaAppMonEnforcementFlowSourceIP
   alaAppMonEnforcementFlowDestIPType
   alaAppMonEnforcementFlowDestIP
   alaAppMonEnforcementFlowSrcPort
   alaAppMonEnforcementFlowDestPort
   alaAppMonEnforcementFlowProtocol
   alaAppMonEnforcementFlowAppName
   alaAppMonEnforcementFlowAppGrpName
   alaAppMonEnforcementFlowPolicyRule
   alaAppMonEnforcementFlowStartTime
   alaAppMonEnforcementFlowPktCount
   alaAppMonEnforcementFlowByteCount
```

show app-mon ipv6-flow-table

Displays the flow table for IPv6 flows entries for enforcement and monitor flows.

show app-mon ipv6-flow-table {monitor | enforcement [verbose]} [{src-ipv6 | dest-ipv6} *ip_address*] **[app-name** *app_name* **| app-group** *grp_name*]

Syntax Definitions

verbose	Displays detailed information of the flows.
src-ipv6 *ip_address*	Filter flow table based on the specified source IPv6 address.
dest-ipv6 *ip_address*	Filter flow table based on the specified destination IPv6 address.
app_name	Filter flow table based on application name.
grp_name	Filter flow table based on application group.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

The **verbose** option displays additional information about the flow start time, statistics counters, associated application group, policy rule, and so on. This option is supported only for enforcement feature.

Examples

```
-> show app-mon ipv6-flow-table monitor
SrcIP            DestIP      SrcPort  DstPort Proto    App Name      App-Group
--------------+------------+--------+-------+-------+-----------+---------------
1000::14        2000::11      58108    80      TCP     youtube        test
1000::14        2000::11      58364    80      TCP     youtube        test
1000::14        2000::11      57085    80      TCP     youtube        test
1000::14        2000::11      57341    80      TCP     youtube        test
1000::14        2000::11      57597    80      TCP     youtube        test
.
.
.

-> show app-mon ipv6-flow-table monitor src-ipv6 1000::11
SrcIP            DestIP      SrcPort  DstPort Proto    App Name      App-Group
--------------+------------+--------+-------+-------+-----------+---------------
1000::14        2000::11      58108    80      TCP     youtube        test
1000::14        2000::11      58364    80      TCP     youtube        test
1000::14        2000::11      57085    80      TCP     youtube        test
1000::14        2000::11      57341    80      TCP     youtube        test
1000::14        2000::11      57597    80      TCP     youtube        test
Number of flows : 5
```

```
-> show app-mon ipv6-flow-table monitor dest-ipv6 2000::11
SrcIP            DestIP      SrcPort  DstPort Proto    App Name      App-Group
-------------+------------+--------+-------+-------+-----------+---------------
1000::14        2000::11      58108    80      TCP     youtube        test
1000::14        2000::11      58364    80      TCP     youtube        test
1000::14        2000::11      57085    80      TCP     youtube        test
1000::14        2000::11      57341    80      TCP     youtube        test
1000::14        2000::11      57597    80      TCP     youtube        test
Number of flows : 5

-> show app-mon ipv6-flow-table monitor app-group test
SrcIP            DestIP      SrcPort  DstPort Proto    App Name      App-Group
-------------+------------+--------+-------+-------+-----------+---------------
1000::14        2000::11      58108    80      TCP     youtube        test
1000::14        2000::11      58364    80      TCP     youtube        test
1000::14        2000::11      57085    80      TCP     youtube        test
1000::14        2000::11      57341    80      TCP     youtube        test
1000::14        2000::11      57597    80      TCP     youtube        test
Number of flows : 5
```

output definitions

SrcIP	Displays flow table based on the specified source IPv6 IP address.
DestIP	Displays flow table based on the specified destination IPv6 IP address.
SrcPort	Displays the flow table based on the source port.
DstPort	Displays the flow table based on the destination port.
Proto	Displays the flow table based on the protocol type.
App Name	Displays the flow table based on the application name.
App-Group	Displays the flow table based on the application group.

```
-> show app-mon ipv6-flow-table enforcement
Src IP                    Dest IP                         App Name
--------------------+-----------------------------+--------------------
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
.
.
.

-> show app-mon ipv6-flow-table enforcement src-ipv6 1000::14
Src IP                    Dest IP                         App Name
--------------------+-----------------------------+--------------------
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
1000::14                  2000::11                        youtube
```

```
-> show app-mon ipv6-flow-table enforcement verbose
Legend: start/date/time/zone   duration
SrcIp      DestIP  SrcPort DestPort Protocol Application-name App-group   Policy Rule   Packet Count Byte Count
-------------------------------------------------------------------------------------------------------------
2015-10-11/16:48:55/IST   0d 0h 3m 0s
1000::11  2000::11 61184   80        TCP      youtube          -         appmon-youtube  61           47437
2015-10-11/16:48:56/IST   0d 0h 2m 59s
1000::11  2000::11 61185   80        TCP      youtube          -         appmon-youtube  31           23696
2015-10-11/16:48:57/IST   0d 0h 2m 58s
1000::11  2000::11 61186   80        TCP      youtube          -         appmon-youtube  4            1430
2015-10-11/16:48:58/IST   0d 0h 2m 57s
1000::11  2000::11 61187   80        TCP      youtube          -         appmon-youtube  61           47437
.
.
.
```

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config	Displays the global AppMon configuration, which includes information about admin-state, running mode, IP mode, aging-timer, and total signatures.

MIB Objects

alaAppMonFlowTable

- alaAppMonFlowSourceIPType
- alaAppMonFlowSourceIP
- alaAppMonFlowDestIPType
- alaAppMonFlowDestIP
- alaAppMonFlowSrcPort
- alaAppMonFlowDestPort
- alaAppMonFlowProtocol
- alaAppMonFlowAppName

alaAppMonEnforcementFlowTable

- alaAppMonEnforcementFlowSourceIPType
- alaAppMonEnforcementFlowSourceIP
- alaAppMonEnforcementFlowDestIPType
- alaAppMonEnforcementFlowDestIP
- alaAppMonEnforcementFlowSrcPort
- alaAppMonEnforcementFlowDestPort
- alaAppMonEnforcementFlowProtocol
- alaAppMonEnforcementFlowAppName
- alaAppMonEnforcementFlowAppGrpName
- alaAppMonEnforcementFlowPolicyRule
- alaAppMonEnforcementFlowStartTime
- alaAppMonEnforcementFlowPktCount
- alaAppMonEnforcementFlowByteCount

show app-mon l4port-exclude

Displays the port range excluded from AppMon operation.

show app-mon l4port-exclude range-id [*number***]**

Syntax Definitions

number	A range ID number. The valid range is 1–8.

Defaults

By default, information is displayed for all range ID numbers.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

Enter a range ID number with this command to display information for a specific range.

Examples

```
-> show app-mon l4port-exclude range-id
Range-Id     Start-port     End-port      Port-type
----------+------------+--------------+----------
1             100           200           UDP-Port
2             20            25            TCP-Service-Port

-> show app-mon l4port-exclude range-id 1
Range-Id     Start-port     End-port      Port-type
----------+------------+--------------+----------
1             100             200         UDP-Port
```

output definitions

Range-Id	The service port range ID.
Start-port	The start port associated with the range ID.
End-port	The end port associated with the range ID.
Port-type	Indicates the port type (**TCP** or **UDP**)

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon l4port-exclude	Configures the L4 port range to exclude from the AppMon operation.

MIB Objects

```
alaAppMonEnforcementL4PortRangeTable
   alaAppMonEnforcementL4PortRangeID
   alaAppMonEnforcementL4PortRangeStart
   alaAppMonEnforcementL4PortRangeEnd
   alaAppMonEnforcementL4PortType
   alaAppMonEnforcementL4PortStatus
```

show app-mon stats

Displays the number of flow statistics.

show app-mon stats

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

Use the **app-mon flow-table enforcement flush** command to clear the counters.

Examples

```
-> show app-mon stats
Chassis/  Total Enforcement Total           Total TCP         Total UDP
Slot      Matched Flows     Used Flows      Overflow Flows    Overflow Packets
--------+----------------+---------------+-----------------+----------------
1/1         8192              8192             1422            0
2/1         0                 3                0               0
3/1         0                 0                0               0
4/1         0                 0                0               0
Total       8192              8195             1422            0
```

output definitions

Chassis/Slot	The chassis ID and slot number.
Total Enforcement Matched Flows	Total number of active flows that matched to any active application signature for enforcement feature.
Total Used Flows	Total number of active flows (including unmatched and enforcement matched) on a given chassis/slot. Each IPv4 flow takes one entry count, while each IPv6 flow takes two entries for Total Used Flows count.
Total TCP Overflow Flows	Total number of TCP flows missed to create flow entry in flow table due to hash collision.
Total UDP Overflow Packets	Cumulative number of UDP packets missed to create flow entry in flow table due to hash collision.

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon flow-table enforcement stats	Enable or disable flow table statistics update for enforcement applications.

MIB Objects

```
alaAppMonStatisticsTable
   alaAppMonStatsSlotIndex
   alaAppMonTotalEnforcementActiveFlows
   alaAppMonTotalFlowTableInUseFlows
   alaAppMonTCPOverflowFlows
   alaAppMonUDPOverflowPackets
```

show app-mon aging enforcement

Displays the aging interval for each application for enforcement feature.

show app-mon aging enforcement [app-name *app_name***]**

Syntax Definitions

app_name	The name of the application. This is a case sensitive string.

Defaults

By default, the aging time for all applications is displayed.

Platforms Supported

OmniSwitch 6860

Usage Guidelines

N/A

Examples

```
-> show app-mon aging enforcement
AppId    Application-name                      TCP Aging-time/
                                               UDP Aging-time(minutes)
------+--------------------------------------+-------------------------
968        amazon                                 6/1
244        facebook                               6/1
182        sip                                    60/60
183        skype                                  6/1
211        tftp                                   15/15
503        twitter                                6/1
597        viber                                  6/1
890        webex                                  6/1
1093       whatsapp                               6/1
240        youtube                                6/1

-> show app-mon aging enforcement app-name sip
AppId    Application-name                      TCP Aging-time/
                                               UDP Aging-time(minutes)
------+--------------------------------------+-------------------------
182      sip                                    60/60
```

output definitions

AppId	Identity of the application.
Application-name	Name of the application.
TCP Aging-time/UDP Aging-time (minutes)	Aging time configured for the application.

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon aging enforcement	Configures the aging time for dynamically learned flows for each application for enforcement feature.

MIB Objects

```
alaAppMonEnforcementAgingTimerTable
   alaAppMonEnforcementAgingTimerAppName
   alaAppMonEnforcementAgingTimerValue
```

show app-mon vc-topology

Displays the AppMon virtual chassis topology.

show app-mon vc-topology

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

Displays the topology of the available OmniSwitch 6860 and OmniSwitch 6860E chassis. This also displays the connectivity between the chassis for flow classification.

Examples

```
-> show app-mon vc-topology
Chassis/    Node            Designated
Slot        Type            Chassis/Slot
--------+----------------+----------------
1/1         OS6860             2/1
2/1         OS6860E            2/1
3/1         OS6860E            3/1
```

output definitions

Chassis/Slot	The chassis ID and slot number.
Node Type	Indicates the switch type.
Designated Chassis/Slot	The chassis and slot of the switch.

Release History

Release 8.2.1; command introduced

Related Commands

N/A

MIB Objects

```
alaAppMonVCTopologyTable
   alaAppMonVCTopologyChassisIndex
   alaAppMonVCTopologyChassisType
   alaAppMonVCTopologyDesignatedChassisIndex
```

clear app-mon app-list

Removes all applications from the enforcement or monitor application list.

clear app-mon app-list {monitor| enforcement}

Syntax Definitions

monitor	Removes all applications from the monitor application list.
enforcement	Removes all applications from the enforcement application list.

Defaults

N/A

Platforms Supported

OmniSwitch 6860

Usage Guidelines

This command does not clear the active application list until the **app-mon apply** command is used.

Examples

```
-> clear app-mon app-list enforcement
-> clear app-mon app-list monitor
```

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon app-list	Add or remove applications or application groups to an application list for enforcement or monitoring.

MIB Objects

```
alaAppMonClearAppList
```

41 Application Fingerprinting Commands

The OmniSwitch Application Fingerprinting feature attempts to detect and identify remote applications by scanning IP packets and comparing them to pre-defined bit patterns (application signatures). Once an application is identified, Application Fingerprinting collects and stores information about the application flow in a database on the local switch. Additional configurable options for this feature include the ability to apply QoS policy list rules to the identified flow and generating SNMP traps when a signature match occurs.

Using this implementation of Application Fingerprinting, an administrator can obtain more detailed information about protocols running on a specific device or make sure that certain QoS actions are automatically applied wherever an application might be running.

MIB information for the Application Fingerprinting commands is as follows:

Filename: ALCATEL-IND1-APP-FINGERPRINT-MIB.mib
Module: alcatelIND1AppFPMIB

A summary of the available commands is listed here:

app-fingerprint admin-state

Enables or disables the Application Fingerprinting process on all Application Fingerprinting ports.

app-fingerprint admin-state {enable | disable}

Syntax Definitions

enable	Enables Application Fingerprinting.
disable	Disables Application Fingerprinting.

Defaults

By default, Application Fingerprinting is enabled for the switch.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When Application Fingerprinting is enabled for the switch, traffic flows on Application Fingerprinting ports are sampled and compared to REGEX application signatures defined in the “app-regex.txt” file located in the **/flash/app-signature** directory on the local switch. This is done to identify the presence of remote applications on a flow-by-flow basis.
- Disabling the administrative status of the Application Fingerprinting feature does not remove the Application Fingerprinting configuration from the switch.

Examples

```
-> app-fingerprint admin-state disable
-> app-fingerprint admin-state enable
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint configuration	Displays the Application Fingerprinting configuration for the switch.

MIB Objects

```
alaAppFPGlobalMIBConfigObjects
   alaAppFPGlobalAdminState
```

app-fingerprint port

Configures a port or link aggregate as an Application Fingerprinting interface. Once the interface is configured and Application Fingerprinting is enabled for the switch, IP packets received on the interface are sampled to determine if they match pre-defined patterns in application signature files that reside on the local switch. When a match occurs, the flow is monitored and/or subject to QoS policy rules.

app-fingerprint {port *chassis/slot/port***[-***port***] | linkagg** *agg_id***[-***agg_id2***]} {monitor-app-group** *group_name* **| policy-list-name** *policy_list* **| unp-profile}**

no app-fingerprint {port *chassis/slot/port***[-***port***] | linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports.
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of ID numbers (5-10).
group_name	The name of an existing signature application group.
policy_list	The name of an existing QoS policy list.
unp-profile	Apply QoS policy list from UNP to which matching traffic is classified.

Defaults

By default, Application Fingerprinting is disabled on all switch ports.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to disable the Application Fingerprinting service on the specified port or link aggregate.
- Use the **monitor-app-group** parameter to specify a group (profile) that represents a set of application signature files. All of the signature files in the group are checked against the IP packets received on the port. When a packet match is detected, the flow is identified and monitored. No other action is taken.
- Use the **policy-list-name** parameter to associate a QoS policy list with the Application Fingerprinting port. When a packet match is detected, the policy rules in the specified policy list are applied to the matching traffic flow.
- Use the **unp-profile** parameter to specify that if traffic received on an Application Fingerprinting interface is classified into a Universal Network Profile (UNP), then the QoS policy list rules associated with that profile are applied to the traffic.
- The QoS policy list specified with the **policy-list-name** parameter or assigned to a UNP for Application Fingerprinting traffic, must contain policy rules with the **appfp-group** condition.
- The QoS policy list specified with the **policy-list-name** parameter must be configured as an **appfp** list. However, the UNP policy list must be configured as a UNP list.

- Application Fingerprinting uses the sFlow mechanism to sample packets. Do not run Application Fingerprinting and other sFlow services on the same port or link aggregate.

Examples

```
-> app-fingerprint port 2/1-5 monitor-app-group my-p2p
-> app-fingerprint linkagg 10 policy-list-name list1
-> app-fingerprint port 1/11 unp
-> no app-fingerprint port 2/1-5
-> no app-fingerprint linkagg 10
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint port	Displays the Application Fingerprinting port configuration.

MIB Objects

```
alaAppFPPortTable
   alaAppFPPort
   alaAppFPGroupNameOrPolicyList
   alaAppFPPortOperationMode
   alaAppFPPortStatus
   alaAppFPPortRowStatus
```

app-fingerprint signature-file

Specifies the name of the Application Fingerprinting signature file. This file contains the REGEX signatures that are used to identify applications accessing the network on Application Fingerprinting ports.

app-fingerprint signature-file *filename*

Syntax Definitions

filename	The name of an existing REGEX application signature file.

Defaults

By default, the “app-regex.txt” file is used.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- This command is only required to use a REGEX signature file that has a filename that is different from the default “app-regex.txt” name..
- The signature file must reside in the **/flash/app-signature** directory on the local switch.
- After specifying the signature filename to use, upload the signature file into the switch memory using the **app-fingerprint reload-signature-file** command.

Examples

```
-> app-fingerprint signature-file app2_regex.txt
```

Release History

Release 7.3.2; command was introduced.

Related Commands

app-fingerprint reload-signature-file	Reloads the contents of the active application signature file into the switch memory.

MIB Objects

```
alaAppFPGlobalMIBConfigObjects
   alaAppFPGlobalSignatureFile
```

app-fingerprint reload-signature-file

Reloads the contents of the active application signature file into the switch memory. Use this command after making any changes to the current signature file.

app-fingerprint reload-signature-file

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- This command reloads the application signature file that was previously applied to the switch. This may be the default “app-regex.txt” file or another signature file that was applied through the **app-fingerprint signature-file** command.
- A switch reboot is *not* required after the signature file is reloaded.

Examples

```
-> app-fingerprint reload-signature-file
```

Release History

Release 7.3.2; command was introduced.

Related Commands

app-fingerprint signature-file Specifies a different signature file to use for Application Fingerprinting.

MIB Objects

```
alaAppFPGlobalMIBConfigObjects
   alaAppFPGlobalReloadSignatureFile
```

app-fingerprint trap

Enables or disables trap generation for the Application Fingerprinting feature.

app-fingerprint trap {enable | disable|

Syntax Definitions

enable	Enables Application Fingerprinting traps.
disable	Disables Application Fingerprinting traps.

Defaults

By default, traps are disabled for this feature.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

A trap is generated when a traffic flow matches an application signature.

Examples

```
-> app-fingerprint trap enable
-> app-fingerprint trap disable
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint configuration	Displays the Application Fingerprinting status and configuration for the switch.

MIB Objects

```
alaAppFPGlobalMIBConfigObjects
alaAppFPGlobalTrapConfig
```

show app-fingerprint configuration

Displays the Application Fingerprinting status and configuration information for the switch.

show app-fingerprint configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show app-fingerprint configuration

Admin-state:          Enabled,
SNMP Trap:            Disabled,
Signature File:       app-regex.txt
```

output definitions

Admin-state	The administrative status of Application Fingerprinting for the switch (**Enabled** or **Disabled**). Configured through the **app-fingerprint admin-state** command.
SNMP Trap	The status of SNMP trap generation for the switch (**Enabled** or **Disabled**). Configured through the **app-fingerprint trap** command.
Signature File	The name of the text file that contains the REGEX application signatures used to identify traffic flows. This file resides in the **/flash/app-signature** directory on the switch. Configured through the **app-fingerprint signature-file** and **app-fingerprint reload-signature-file** commands.

Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint port	Displays the Application Fingerprinting port configuration.

MIB Objects

```
alaAppFPGlobalMIBConfigObjects
   alaAppFPGlobalAdminState
   alaAppFPGlobalSignatureFile
   alaAppFPGlobalReloadSignatureFile
   alaAppFPGlobalTrapConfig
```

show app-fingerprint port

Displays the Application Fingerprinting port configuration for the switch.

show app-fingerprint [port *chassis/slot/port* **| linkagg** *agg_id***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port***]**	The slot and port number (3/1).
agg_id	The link aggregate ID number.

Defaults

By default, the configuration for all Application Fingerprinting ports is displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **port** and **linkagg** parameters to display information for a specific port or link aggregate.

Examples

```
-> show app-fingerprint port
Legend: * = Port or App-Group is invalid

  Port    Operation Mode          App-group/Policy-list
--------+---------------+---------------------------------------
1/2/1     Monitoring        Testing13
1/2/1     QoS               list1
1/2/1     QoS               list2

-> show app-fingerprint linkagg
Legend: * = Port or App-Group is invalid

  Port    Operation Mode          App-group/Policy-list
--------+---------------+---------------------------------------
0/100     Monitoring        Testing16
0/100     QoS               list3
0/100     QoS               list4
```

output definitions

Port	The slot/port or link aggregate ID of the Application Fingerprinting interface. A “0” slot number indicates that the interface is a link aggregate.
Operation Mode	The Application Fingerprinting mode (**Monitoring**, **QoS**, or **UNP**) in which the port is operating.
App-group/Policy-list	The name of the group of application signatures or the QoS policy list that is applied to the traffic flows on the port.

Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint port	Displays the Application Fingerprinting interface configuration.
show app-fingerprint configuration	Displays the Application Fingerprinting status and configuration for the switch.

MIB Objects

```
alaAppFPPortTable
   alaAppFPPort
   alaAppFPGroupNameOrPolicyList
   alaAppFPPortOperationMode
   alaAppFPPortStatus
   alaAppFPPortRowStatus
```

show app-fingerprint app-name

Displays the REGEX application signature configuration for the switch. When the switch samples Application Fingerprinting ports, the traffic flow patterns on these ports are compared against the REGEX signatures specified in the “app-regex.txt” file. When a match occurs, the traffic flow is classified and monitored. In addition, QoS policies can be applied to these flows based on a specific match to an application signature group.

show app-fingerprint app-name [*app_name***]**

Syntax Definitions

app_name	The name of an existing application signature.

Defaults

By default, all application signatures are displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Application signatures are defined in the “app-regex.txt” file that resides in the **/flash/app-signature** directory on the switch. A default version of this file is available, but the file is user-configurable and new files can also be created.
- Application signatures can also be combined into an application group. This type of group is then assigned to one or more Application Fingerprinting ports. All the application signatures that are members of the assigned group are then applied to traffic flows on that same port.
- Use the *app_name* parameter to display information for a specific application signature.

Examples

```
-> show app-fingerprint app-name
App Name: ciscovpn
  Description: VPN client software to a Cisco VPN server
  REGEX Signature: \x01\xf4\x01\xf4

App Name: citrix
  Description: Citrix ICA - proprietary remote desktop application
  REGEX Signature: \x32\x26\x85\x92\x58

App Name: dhcp
  Description: Dynamic Host Configuration Protocol
  REGEX Signature: [\x01\x02][\x01- ]\x06.*c\x82sc

-> show app-fingerprint app-name citrix

App Name: citrix
  Description: Citrix ICA - proprietary remote desktop application
  REGEX Signature: \x32\x26\x85\x92\x58
```

output definitions

App-name	The name of the application for which this signature applies.
Description	A description of the application.
REGEX signature	The regular expression (REGEX) that identifies this application.

Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint app-group	Displays the application group configuration.
show app-fingerprint configuration	Displays the Application Fingerprinting status and configuration.

MIB Objects

```
alaAppFPAppGrpNameTable
   alaAppFPGrpAppName
```

show app-fingerprint app-group

Displays the Application Fingerprinting application group configuration for the switch. An application group contains a user-configured list of REGEX application signatures that are represented by the group name. The group name is then assigned to Application Fingerprinting ports or link aggregates.

show app-fingerprint app-group [*group_name***]**

Syntax Definitions

group_name	The name of an existing application group.

Defaults

By default, all application groups are displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Application groups are defined in the “app-regex.txt” file that is located in the **/flash/app-signature** directory on the switch. A default version of this file is available, but the file is user-configurable and new files can also be created.
- Use the *group_name* parameter to display information for a specific application group.

Examples

```
-> show app-fingerprint app-group

App Group: chatting
  App names: jabber

App Group: mail
  App names: smtp

App Group: network
  App names: bgp dhcp rtsp smb

App Group: p2p
  App names: hotline

App Group: remote_access
  App names: ciscovpn citrix rdp ssh vnc

App Group: voip
  App names: h323 sip

-> show app-fingerprint app-group network

App Group: network
  App names: bgp dhcp rtsp smb
```

output definitions

App-Group	The name of the application group file.
App names	The names of the application signature files that belong to this group.

Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint app-name	Displays the contents of the REGEX application signatures that are stored in the “app-regex.txt” file on the switch.
show app-fingerprint configuration	Displays the Application Fingerprinting status and configuration.

MIB Objects

```
alaAppFPAppGrpNameTable
   alaAppFPAppGroupName
   alaAppFPGrpAppName
```

show app-fingerprint database

Displays Application Fingerprinting database entries. When a match occurs between an IP traffic flow and a REGEX application signature, a multi-tuple classifier and the name of the matching application group and signature are stored in a local switch database to identify and track the application associated with the flow.

show app-fingerprint database [port *chassis/slot/port* **| linkagg** *agg_id***] [detail]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and the port number (3/1).
agg_id	The link aggregate ID number.
detail	Displays additional information about the classified traffic flow.

Defaults

By default, all application flow database entries are displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **port** and **linkagg** parameters to display information for a specific port or link aggregate.
- The following multi-tuple classifier is used to identify an application traffic flow:
  - Ingress Port
  - Dest MAC
  - Src MAC
  - VLAN
  - Dest IP
  - Src IP
  - Dest Port
  - Src Port
- Each database entry is subject to a 15 minute aging period. If the database fills up, older entries are aged out before the 15 minute limit (fast aging). However, fast aging is not applied to database entries associated with QoS. In this case, the QoS is removed after the regular 15 minute aging time period expires.
- When a database entry is removed due to regular aging or fast aging conditions, any corresponding QoS is also removed for that flow.

Examples

```
-> show app-fingerprint database

Port   App-Group/Name       SRC MAC        VLAN   SRC IP/Port
-----+----------------+-----------------+------+--------------
0/1/2  P2P/aim          00:00:22:33:44:55    20    2.3.4.4/200
0/1/2  P2P/ares         00:00:22:33:44:55    20    2.3.4.4/200
0/1/2  Mail/smtp        00:00:22:33:44:55    20    2.3.4.4/100
```

output definitions

Port	The slot/port or link aggregate ID of the AFP interface on which the flow was classified. A “0” slot number indicates a link aggregate.
App-Group/Name	The name of the application group and signature that matched the flow.
SRC MAC	The source MAC address of the flow.
VLAN	The VLAN on which the flow is learned and forwarded.
SRC IP/Port	The source IP network address and port.

```
-> show app-fingerprint database detail
Port 1/2/1:
    App-Group/Name: Testing2/App_4
      SRC-DST MAC:    00:00:00:00:04:01  -  00:e0:b1:e6:f9:b5,
      VLAN:           20,
      SRC IP/PORT:    20.20.20.21/65,
      DST IP/PORT:    10.10.10.11/55

    App-Group/Name: Testing2/App_5
      SRC-DST MAC:    00:00:00:00:04:02  -  00:e0:b1:e6:f9:b5,
      VLAN:           20,
      SRC IP/PORT:    20.20.20.21/64,
      DST IP/PORT:    10.10.10.11/54

    App-Group/Name: Testing2/App_6
      SRC-DST MAC:    00:00:00:00:04:03  -  00:e0:b1:e6:f9:b5,
      VLAN:           20,
      SRC IP/PORT:    20.20.20.21/66,
      DST IP/PORT:    10.10.10.11/56

Port 2/3/23:
    App-Group/Name: Testing1/App_1
      SRC-DST MAC:    00:00:00:00:03:01  -  00:e0:b1:e6:f9:b5,
      VLAN:           10,
      SRC IP/PORT:    10.10.10.11/115,
      DST IP/PORT:    20.20.20.21/137

    App-Group/Name: Testing1/App_2
      SRC-DST MAC:    00:00:00:00:03:02  -  00:e0:b1:e6:f9:b5,
      VLAN:           10,
      SRC IP/PORT:    10.10.10.11/114,
      DST IP/PORT:    20.20.20.21/138

    App-Group/Name: Testing1/App_3
      SRC-DST MAC:    00:00:00:00:03:03  -  00:e0:b1:e6:f9:b5,
      VLAN:           10,
      SRC IP/PORT:    10.10.10.11/113,
      DST IP/PORT:    20.20.20.21/135
```

output definitions

Port	The slot and port number on which the flow was classified.
App-Group/Name	The name of the application group and signature that matched the flow.
SRC-DST MAC	The source and destination MAC addresses of the flow.
VLAN	The VLAN on which the flow is learned and forwarded.
SRC IP/Port	The source IP network address and port.
DST IP/Port	The destination IP network address and port.

Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint app-group	Displays the application group configuration.
show app-fingerprint configuration	Displays the Application Fingerprinting status and configuration.

MIB Objects

```
alaAppFPDatabaseTable
   alaAppFPDbPort
   alaAppFPDbAppGroupName
   alaAppFPDbAppName
   alaAppFPDbSrcMacAddr
   alaAppFPDbVlanId
   alaAppFPDbSrcIpAddrType
   alaAppFPDbSrcIpAddr
   alaAppFPDbSrcPort
   alaAppFPDbDstIpAddrType
   alaAppFPDbDstIpAddr
   alaAppFPDbDstPort
   alaAppFPDbDstMacAddr
```

show app-fingerprint statistics

Displays statistics for each application flow on an Application Fingerprinting ingress port.

show app-fingerprint statistics [port *chassis/slot/port* **| linkagg** *agg_id***]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot and the port number (3/1).
agg_id	The link aggregate ID number.

Defaults

By default, statistics are displayed for all application flows.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **port** and **linkagg** parameters to display information for a specific port or link aggregate.
- Statistics displayed with this command include total number of packets matched, the number of unmatched packets, and the packets matched for each application signature.

Examples

```
-> show app-fingerprint statistics
   Port    Group/App name                                Last 1 hour       Last 1 day
---------+---------------------------------------------+---------------+----------------
1/2/1     Testing2/App_4                                        19976        19976
1/2/1     Testing2/App_5                                        20000        20000
1/2/1     Testing2/App_6                                        20000        20000
2/3/23    Testing1/App_1                                        19975        19975
2/3/23    Testing1/App_2                                        20000        20000
2/3/23    Testing1/App_3                                        20000        20000
```

Release History

Release 7.3.2; command introduced.

Related Commands

show app-fingerprint port	Displays the Application Fingerprinting interface configuration.

MIB Objects

```
alaAppFPStatsTable
   alaAppFPStatsPort
   alaAppFPStatsGroupName
   alaAppFPStatsAppName
   alaAppFPTotalMatchedLast1Hour
   alaAppFPTotalMatchedLast1Day
```

42 FIP Snooping Commands

The OmniSwitch implementation of Fibre Channel over Ethernet (FCoE) Initiation Protocol (FIP) snooping supports the FCoE technology used to tunnel Fibre Channel (FC) frames within Ethernet MAC frames.When the FCoE and FIP snooping functionality is enabled, the OmniSwitch serves as an FCoE transit switch. In this role, the OmniSwitch implementation of Data Center Bridging (DCB) is also used to provide the lossless Ethernet network required to support FCoE.

This implementation of FIP snooping ensures the security of the FCoE network and maintains a virtual point-to-point network connection between FCoE Nodes (ENodes) and FCoE Forwarder (FCF) devices. In addition, FIP snooping is also required to support OmniSwitch FCoE/FC gateway functionality that allows the switch to provide FCoE forwarding services between an FCoE network and a native FC storage area network (SAN).

- An OmniSwitch FCoE transit switch is placed between ENodes (servers or other bridges) and an FCF or an OmniSwitch FCoE/FC gateway to extend the reach of the FCoE network without extending the physical FC connections.
- An OmniSwitch FCoE/FC gateway runs FIP snooping on the 10G Ethernet FCoE ports that connect to an FCoE network. On the same switch, FC ports connect to native FC switches or nodes. Traffic is transmitted between the FCoE network and the FC SAN through the gateway switch.

This chapter provides information about configuring FCoE and FIP global and port parameters through the Command Line Interface (CLI). See Chapter 43, “FCoE/FC Gateway Commands,” for more information about configuring OmniSwitch FCoE/FC gateway functionality.

MIB information for the FCoE and FIP snooping commands is as follows:

Filename: ALCATEL-IND1-FIPS-MIB.mib
Module: alcatelIND1FipsMIB

The FCoE and FIP Snooping commands are listed here:

Global commands	**fcoe fip-snooping** **fcoe address-mode** **fcoe priority** **fcoe priority-protection** **fcoe priority-protection action** **fcoe filtering-resource trap-threshold** **fcoe house-keeping-time-period**
VLAN and Port commands	**fcoe vlan** **fcoe fcf mac** **fcoe fc-map** **fcoe discovery-advertisement** **fcoe role**

Show commands	**show fcoe** **show fcoe ports** **show fcoe sessions** **show fcoe enode** **show fcoe fcf** **show fcoe fc-map** **show fcoe discovery-advertisement**
Statistics commands	**show fcoe statistics** **clear fcoe statistics**

fcoe fip-snooping

Enables or disables Fibre Channel Initiation Protocol (FIP) snooping on the switch. FIP Snooping is enabled to allow the OmniSwitch to serve as an FCoE transit switch.

fcoe fip-snooping admin-state {enable | disable}

Syntax Definitions

enable	Enables FIP Snooping.
disable	Disables FIP Snooping.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

When FIP Snooping is enabled, traffic with an Ethertype of FCoE is dropped on all switch VLANs and ports that are not configured as FCoE VLANs and ports.

Examples

```
-> fcoe fip-snooping admin-state enable
-> fcoe fip-snooping admin-state disable
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show fcoe	Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

```
alaFipsConfig
   alaFipsConfigFIPSAdmin
```

fcoe address-mode

Configures the FCoE addressing mode. This mode determines whether a server-provided MAC address (SPMA) or a fabric-provided MAC address (FPMA) is assigned to virtual FCoE entities.

fcoe address-mode {spma | fpma}

Syntax Definitions

spma	Selects the SPMA address mode.
fpma	Selects the FPMA address mode.

Defaults

parameter	default
spma | fpma	FPMA

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The FCoE Node (ENode) and the FCoE Forwarder (FCF) must use the same addressing mode to establish virtual links between the ENode and FCF. Configure the global OmniSwitch addressing mode to match the mode used by the ENode and FCF.
- When the FPMA mode is active, a MAC address is assigned by an FCF to a single ENode MAC. This MAC address is not assigned to any other ENode MAC in the same VLAN.
- When the SPMA mode is active, MAC addresses are assigned by the ENode server.
- To change the addressing mode selection, disable FIP Snooping for the switch then make the change and enable FIP Snooping again.

Examples

```
-> fcoe address-mode spma
-> fcoe address-mode fpma
```

Release History

Release 7.3.2; command was introduced.

Related Commands

fcoe fip-snooping	Enables or disables FIP Snooping on the switch
show fcoe	Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

```
alaFipsConfig
   alaFipsConfigAddressMode
```

fcoe priority

Configures up to two global priority values that are designated as lossless for FCoE traffic.

fcoe priority {*priority***} [***priority***]**

Syntax Definitions

priority	A priority value between 0–7.

Defaults

parameter	default
priority	3

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- This command overwrites the existing FCoE priority values used by the switch.
- If two priority values are configured but there is a need to change only one of the values, both priority values must be specified with this command. For example, if the current priority is set to 2 and 5, to change priority 2 to 3, specify both 3 and 5 as the priority values.
- Specify a priority value of 3 to set the priority back to the default value.
- The FCoE priority values are used when FCoE priority protection is enabled for the switch.
- In addition to enabling priority protection, a lossless DCB FCoE profile with the same FCoE priority values must be assigned to the FCoE interfaces.

Examples

```
-> fcoe priority 2 5
-> fcoe priority 3 5
-> fcoe priority 3
```

Release History

Release 7.3.2; command was introduced.

Related Commands

fcoe priority-protection	Configures the status of priority protection for the switch.
fcoe priority-protection action	Configures the action taken when traffic is not FCoE or FIP.
fcoe fip-snooping	Enables or disables FIP Snooping on the switch
show fcoe	Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

```
alaFipsConfig
   alaFipsConfigPriorityOne
   alaFipsConfigPriorityTwo
```

fcoe priority-protection

Enables or disables priority protection.

fcoe priority-protection {enable | disable}

Syntax Definitions

enable	Enables priority protection for the switch.
disable	Disables priority protection for the switch.

Defaults

By default, priority protection is disabled for the switch.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When priority protection is enabled, only FCoE and FIP traffic that matches the FCoE lossless priority values is allowed. All other traffic is either marked or dropped, based on the priority protection action configured for the switch.
- This command applies only to the priority value that is specified using the **fcoe priority** command.
- The FCoE priority value is advertised to FCoE-enabled hosts using the Data Center Bridging Exchange (DCBx) protocol.

Examples

```
-> fcoe priority-protection enable
-> fcoe priority-protection disable
```

Release History

Release 7.3.2; command was introduced.

Related Commands

fcoe priority	Configures the lossless priority values for the switch.
fcoe priority-protection action	Determines whether non-FCoE and non-FIP traffic is dropped or marked with a lower priority value.
fcoe fip-snooping	Enables or disables FIP Snooping on the switch
show fcoe	Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

```
alaFipsConfig
   alaFipsConfigPrioProtection
```

fcoe priority-protection action

Specifies whether non-FCoE and non-FIP traffic is dropped or marked with a lower priority value. This action is only valid when FCoE priority protection is enabled for the switch.

fcoe priority-protection action {drop | remark *priority***}**

Syntax Definitions

drop	All non-FCoE and non-FIP traffic is dropped.
priority	Specifies the priority value to use for remarking non-FCoE and non-FIP traffic.

Defaults

By default, non-FCoE and non-FIP traffic is dropped when priority protection is enabled for the switch.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When priority protection is enabled, only FCoE traffic that matches the protected priority values is allowed in the priority queues. All other traffic is either re-marked or dropped, based on the priority protection action configured for the switch.
- If the re-mark action is configured, traffic is marked with the specified priority value and forwarded on the switch.

Examples

```
-> fcoe priority-protection action drop
-> fcoe priority-protection action remark 0
```

Release History

Release 7.3.2; command was introduced.

Related Commands

fcoe priority	Configures the lossless priority values for the switch.
fcoe priority-protection	Configures the status of priority protection for the switch
fcoe fip-snooping	Enables or disables FIP Snooping on the switch
show fcoe	Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

```
alaFipsConfig
   alaFipsConfigPriorityProtectionAction
```

fcoe filtering-resource trap-threshold

Configures the percentage of filtering resources used as a trap threshold value. When this percentage is reached, a trap is generated by the switch.

fcoe filtering-resource trap-threshold *percentage*

Syntax Definitions

percentage	The percentage of filtering resources used.

Defaults

By default, the filtering resource trap threshold percentage is set to 80%.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

To disable the generation of filtering resource traps, set the trap threshold value to “0”.

Examples

```
-> fcoe filtering-resource trap-threshold 50
-> fcoe filtering-resource trap-threshold 0
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show fcoe	Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

```
Notifications (Traps)
   alaFipsResourceThresholdReached
   alaFipsFilterResourceUsage
```

fcoe house-keeping-time-period

Configures the amount of time the FCoE switch waits to receive keep alive messages from the ENode and FCF for a given FCoE session. When this time expires and no keep alive messages were received for any entity of the session, the session information is removed.

fcoe house-keeping-time-period *seconds*

Syntax Definitions

seconds	The keep alive wait time, in seconds.

Defaults

By default, the housekeeping timer is set to 300 seconds.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

To disable the housekeeping timer, set the timer value to “0”

Examples

```
-> fcoe house-keeping-time-period 120
-> fcoe house-keeping-time-period 0
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show fcoe	Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

```
alaFipsConfig
   alaFipsConfigHouseKeepingTimePeriod
```

fcoe vlan

Configures an FCoE VLAN. This type of VLAN is used to deploy the OmniSwitch implementation of FIP snooping.

fcoe vlan *vlan_id* **[admin-state {enable | disable}] [name** *description***]**

no fcoe vlan *vlan_id*

Syntax Definitions

vlan_id	A numeric value that uniquely identifies an individual FCoE VLAN. The valid ID range is 2–4094.
enable	Enables the FCoE VLAN administrative status.
disable	Disables the FCoE VLAN administrative status.
description	An alphanumeric string. Optional name description for the VLAN ID. Enclose the description in double quotes if it contains more than one word with a space in between.

Defaults

parameter	default
enable | disable	**enable**
description	**VLAN ID**

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a FCoE VLAN from the switch configuration. All VLAN ports are detached before the VLAN is removed.
- Specify a VLAN ID that does not exist in the switch configuration, or the ID of a dynamically created MVRP VLAN.
- Only 802.1q-tagged FCoE ports and link aggregates can be members of FCoE VLANs.
- Configuring a FCoE VLAN as a default VLAN for a port or link aggregate is not allowed. All port associations are created by tagging FCoE ports with the FCoE VLAN ID.
- Configuring default VLAN 1 as an FCoE VLAN is not allowed.

- The following features are not supported on FCoE VLANs:
  - IGMP Snooping
  - IP interface
  - HA VLANs
  - SVLAN and CVLAN
  - Shortest Path Bridging (SPB)
  - MCLAG
  - UDP Relay, DHCP Snooping
  - Universal Network Profile (UNP)
- An OmniSwitch FCoE transit switch operates between an FCoE Node (ENode) and a FCoE Forwarder (FCF). Manual configuration of the FCoE VLAN is required along the transit switch path. However, the ENode and FCF may invoke FIP VLAN discovery to discover the FCoE VLANs within the transit path. If not, manual configuration of the FCoE VLANs may also be required on the appropriate ENodes and FCFs.

Examples

```
-> fcoe vlan 100
-> no fcoe vlan 100
-> fcoe vlan 100 admin-state enable name fcoe-vlan1
-> fcoe vlan 100 admin-state enable
```

Release History

Release 7.3.2; command introduced.

Related Commands

fcoe fcf mac	Configures a static Fibre Channel Forwarder (FCF) MAC address for the specified FCoE VLAN.
fcoe fip-snooping	Enables or disables FIP Snooping on the switch
show vlan	Displays the VLAN configuration for the switch.

MIB Objects

```
alaFipsVlanTable
   alaFipsVlanId
   alaFipsVlanFCMap
   alaFipsVlanRowStatus
```

fcoe fcf mac

Configures a static Fibre Channel Forwarder (FCF) MAC address for the specified FCoE VLAN. Virtual Fibre Channel (FC) links that traverse the lossless Ethernet network send FCoE frames to and from the FCF MAC address.

fcoe fcf mac *mac_address* **vlan** *vlan_id*

no fcoe fcf *mac_address* **vlan** *vlan_id*

Syntax Definitions

mac_address	Enter the FCF MAC Address (for example, 00:00:39:59:f1:0c).
vlan_id	An existing FCoE VLAN ID. The valid ID range is 2–4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the FCF MAC address from the specified FCoE VLAN.
- The FCoE VLAN ID must already exist in the switch configuration.

Examples

```
-> fcoe fcf mac 30:10:94:01:00:00 vlan 100
-> no fcoe fcf 30:10:94:01:00:00
```

Release History

Release 7.3.2; command introduced.

Related Commands

fcoe vlan	Configures an FCoE VLAN for the switch.
fcoe fip-snooping	Enables or disables FIP Snooping on the switch
show vlan	Displays the VLAN configuration for the switch.

MIB Objects

```
alaFipsVlanTable
   alaFipsVlanId
   alaFipsVlanFCMap
```

fcoe fc-map

Configures a static Fibre Channel Mapped Address Prefix (FC-MAP) for the specified FCoE VLAN. The FC-MAP is a 24-bit value used by the Fibre Channel Forwarder (FCF) to identify an individual fabric.

fcoe fc-map *prefix* **vlan** *vlan_id*

no fcoe fc-map *prefix* **vlan** *vlan_id*

Syntax Definitions

prefix	Enter the FC-MAP prefix value. The valid range is 0EFC00–0EFCFF.
vlan_id	An existing FCoE VLAN ID. The valid ID range is 2–4094.

Defaults

By default, the FC-MAP is set to 0E:FC:00.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- On an OmniSwitch 6900, use the **no** form of this command to set the FC-MAP back to the default value (0E:FC:00) for the specified FCoE VLAN.
- The FCoE VLAN ID must already exist in the switch configuration.
- The configured FC-MAP value assigned to an FCoE VLAN must match the FC-MAP value used by the FCF device. FCF advertisement packets that contain a different FC-MAP are not processed by the switch.
- When the FCoE address mode is set to Fabric-Provided MAC Address (FPMA), the FCF uses the FC-MAP value (upper 24 bits) combined with an FCID value (lower 24 bits) to generate a unique MAC address to identify an ENode VN_Port for FCoE transactions.

Examples

```
-> fcoe fc-map 0E:FC:04 vlan 30
-> no fcoe fc-map 0E:FC:04 vlan 30
```

Release History

Release 7.3.2; command introduced.

Related Commands

fcoe vlan	Configures an FCoE VLAN for the switch.
fcoe fip-snooping	Enables or disables FIP Snooping on the switch
show vlan	Displays the VLAN configuration for the switch.

MIB Objects

```
alaFipsVlanTable
   alaFipsVlanId
   alaFipsVlanFCMap
```

fcoe discovery-advertisement

Configures FIP discovery advertisement message parameters for the specified FCoE VLAN. These parameter values are advertised in both unicast and multicast advertisements.

fcoe discovery-advertisement vlan *vlan_id***[-***vlan_id2***] [a-bit {enable | disable}] [fka-adv-period** *adv_seconds***] [priority** *priority***] [uds-retries** *retries***]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	An existing FCoE VLAN ID. Use a hyphen to specify a range of FCoE VLAN IDs (10-25).
enable	Enables the available-for-login bit (A-bit) in the discovery advertisement message to indicate that the switch can accept fabric logins from ENodes.
disable	Disables the A-bit in the discovery advertisement message to indicate that the switch cannot accept fabric logins from ENodes.
adv_seconds	The discovery advertisement transmission interval and the number of FIP ENode keep alive packets expected. The valid range is 1–90 seconds.
priority	The priority value assigned to the switch, indicated in the priority descriptor of the discovery advertisement message. The valid range is 0–255 (0 = highest priority, 255 = lowest priority).
retries	The number of times a unicast discovery solicitation is transmitted after a port on which an FCF MAC was learned goes down. The valid range is 0–10.

Defaults

parameter	default
a-bit enable | disable	**enable**
fka-adv-period *acv_seconds*	**8**
priority *priority*	**128**
uds-retries *retries*	**0**

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When the A-bit parameter is disabled, the switch will not process any new logins for the FCoE VLAN. However, there is no impact on existing VN_Port sessions, which are allowed to continue.
- Transmitting unicast discovery solicitations helps to find out if the same FCF is reachable on some other port of the same FCoE VLAN.

Examples

```
-> fcoe discovery-advertisement vlan 100 priority 10
-> fcoe discovery-advertisement uds-retries 3
-> no fcoe discovery-advertisement vlan 100
```

Release History

Release 7.3.3; command introduced.

Related Commands

show fcoe discovery-advertisement	Displays the discovery advertisement parameter values for the specified VLANs.

MIB Objects

```
alaFipsDiscAdvtTable
   alaFipsDiscAdvtVlanId
   alaFipsDiscAdvtAbit,
   alaFipsDiscAdvtFkaAdvPeriod,
   alaFipsDiscAdvtPriority,
   alaFipsDiscAdvtUdsRetries,
   alaFipsDiscAdvtRowStatus
```

fcoe role

Configures the specified port or link aggregate as an FCoE interface and defines the role of the interface in the FCoE network.

fcoe {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]} role {edge | enode-only | fcf-only | mixed | trusted | ve}**

no fcoe {port *chassis/slot/port***[**-*port2***]** | **linkagg** *agg_id***[**-*agg_id2***]}**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8). FCoE is only supported on 10G or faster ports.
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
edge	Port connects directly to an ENode for transmission of FCoE and FIP frames from the ENode to the FCF.
enode-only	Link between FCoE switches that carries traffic from ENode to FCF.
fcf-only	Link between FCoE switches that carries traffic from FCF to ENode.
mixed	Link between FCoE switches that carries traffic in both directions (from FCF to ENode or from ENode to FCF).
trusted	Trust the FCoE Edge port; traffic on this port is not filtered by FIP ACLs. This port role type is typically assigned to the switch FCoE port that connects to an Ethernet port on the FCF.
ve	Configures port as a virtual expansion port (VE_Port) that is associated with an E2E-tunnel session. A VE_Port emulates an E_Port in an FCoE network, providing connectivity between FC switches. VE_Ports discover FCFs.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to revert the FCoE port back to a regular switch port. Before doing so, however, delete any associations the port may have with an FCoE VLAN.
- To change the role of an FCoE port, first remove the FCoE configuration from the port, then configure FCoE and the new role again for that same port.
- FCoE is only supported on 10G or faster ports that are associated with an FCoE lossless DCB profile. In addition, DCBX must be enabled on the port with both PFC and ETS in an active state (either forced

or negotiated via DCBX). The DCB configuration is done separately using QoS port and profile commands.

- The maximum frame size for an FCoE port must be at least 2500 bytes to accommodate FCoE encapsulated frames, which are larger than the standard Ethernet frame size. In addition, make sure the FCoE port frame size is configured the same end-to-end.
- When configuring a link aggregate as an FCoE port, make sure the link aggregate ID number already exists in the switch configuration. Ports already configured as FCoE ports cannot be added to a link aggregate.
- FCoE ports must be manually assigned to a default VLAN and then tagged with the FCoE VLAN that will carry the FCoE and FIP frames on that port.
- The following features are not supported on FCoE ports:
  - Learned Port Security (LPS)
  - Port Mirroring and Remote Port Mirroring
  - Shortest Path Bridging (SPB)
- Enabling FCoE on a Universal Network Profile (UNP) port is only supported to allow UNP dynamic assignment of a default VLAN for an FCoE port. Manual tagging of the FCoE UNP port with FCoE VLAN IDs is still required.
- FCoE VLANs may be dynamically learned through the transmission of MVRP join PDU, but any port associations with that VLAN must be manually configured.
- Assigning FCoE interfaces to different FCoE VLANs provides a method for configuring multiple FC fabrics through the same FCoE switch.

Examples

```
-> fcoe port 1/1 role edge
-> fcoe port 1/1/1 role edge
-> fcoe port 2/1 role fcf-only
-> no fcoe port 2/1
```

Release History

Release 7.3.2; command introduced.

Related Commands

fcoe vlan	Configures an FCoE VLAN.
show fcoe ports	Displays the status and configuration of FCoE interfaces.

MIB Objects

```
alaFipsIntfTable
   alaFipsIntfIfIndex
   alaFipsIntfOperStatus
   alaFipsIntfPortRole
   alaFipsIntfRowStatus
```

show fcoe

Displays the global FCoE and FIP snooping status and configuration information for the switch.

show fcoe

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show fcoe

FCoE Global Configurations:
---------------------------
FIP Snooping              : Disable,
Address-Mode              : FPMA,
Priority 1                : 3,
Priority 2                : -,
Priority Protection       : Enable,
Priority Protection Action: Drop,
Re-Mark Priority          : -,
Total Filter Resources    : 256,
Used Filter Resources     : 0,
Trap threshold (%)        : 80,
House Keeping Time Period : 300
```

output definitions

FIP Snooping	The administrative status of FIP snooping for the switch (**Enable** or **Disable**). Configured through the **fcoe fip-snooping** command.
Address-mode	Indicates whether a server-provided MAC address (**SPMA**) or a fabric-provided MAC address (**FPMA**) is assigned to virtual FCoE entities. Configured through the **fcoe address-mode** command.
Priority 1	One of two global lossless priority values for FCoE traffic. Configured through **fcoe priority** command.
Priority 2	Two of two global lossless priority values for FCoE traffic. Configured through **fcoe priority** command.

output definitions (continued)

Priority Protection	The status of priority protection for the switch (**Enable** or **Disable**). Configured through the **fcoe priority-protection** command.
Priority Protection Action	The action applied to traffic that does not match the FCoE/FIP Ethertype and configured FCoE priority value (**Drop** or **Remark**). Configured through the **fcoe priority-protection action** command.
Re-mark Priority	The priority value to use for marking traffic that does not match the FCoE/FIP Ethertype and configured FCoE priority value. This value is only applied when the priority protection action is set to **Remark**. Configured through the **fcoe priority-protection action** command.
Total Filtering Resources	The number of ACL entries available for filtering of FCoE traffic.
Used Filtering Resources	The number of ACL entries currently in use for filtering FCoE traffic.
Trap threshold (%)	The percentage of filtering resources used for FIP. When this percentage is reached, a trap is sent indicating the available and maximum percentage of filtering resources. Configured through the **fcoe filtering-resource trap-threshold** command.
House Keeping Time Period	The amount of time the FCoE switch will wait to receive keep alive messages from the ENode and FCF. When this amount of time expires, information for the specific FCoE session is removed. Configured through the **fcoe house-keeping-time-period** command

Release History

Release 7.3.2; command was introduced.

Related Commands

show fcoe ports	Displays the FCoE port configuration for the switch.
show fcoe sessions	Displays the status and configuration of the FIP snooping sessions.

MIB Objects

```
alaFipsConfig
   alaFipsInfo
   alaFipsConfigFIPSAdmin
   alaFipsConfigAddressMode
   alaFipsConfigPriorityOne
   alaFipsConfigPriorityTwo
   alaFipsTotalNumFilterResource
   alaFipsUsedNumFilterResource
   alaFipsConfigHouseKeepingTimePeriod
NOTIFICATIONS (TRAPS)
   alaFipsResourceThresholdReached
```

show fcoe ports

Displays the FCoE interface configuration for the switch.

show fcoe ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

This command also shows the FCoE role assigned to the interface.

Examples

```
-> show fcoe ports
  Ports       FCoE Role       Status
----------+---------------+-----------
 1/3        Edge Port         DISABLE
 1/4        Edge Port         DISABLE
 1/5        Edge Port         DISABLE
 1/6        Edge Port         DISABLE
 1/7        Edge Port         DISABLE
 1/11       Edge Port         DISABLE
 1/13       Edge Port         ENABLED
 1/14       Edge Port         ENABLED
 1/15       Edge Port         DISABLE
 1/19       FCF Port          DISABLE
 2/1        Edge Port         DISABLE
 2/8        Edge Port         DISABLE
 0/1        Mixed Port        DISABLE
 0/12       Mixed Port        ENABLED
 0/40       Mixed Port        DISABLE
 0/50       Mixed Port        ENABLED
```

output definitions

Ports	The slot/port or link aggregate ID of the FCoE interface. A “0” slot number indicates that the FCoE interface is a link aggregate.
FCoE Role	The designated role of the FCoE interface (**Edge Port**, **ENode Port**, **FCF Port**, **Mixed Port**, or **Trusted Port**).
Status	The operational status of the FCoE interface (**ENABLE** or **DISABLE**).

Release History

Release 7.3.2; command was introduced.

Related Commands

fcoe role	Configures a port or link aggregate as an FCoE interface.
show fcoe	Displays the FCoE and FIP status and configuration for the switch.

MIB Objects

```
AlaFipsIntfTable
   alaFipsIntfIfIndex
   alaFipsIntfOperStatus
   alaFipsIntfPortRole
   alaFipsIntfRowStatus
```

show fcoe sessions

Displays the FIP snooping session status and configuration for the switch.

show fcoe sessions [[fips | npiv-proxy | r-npiv] [port *chassis/slot/port***]** | **vlan** *vlan_id* **| linkagg** *agg_id***] | [e-tunnel [***tunnel_id***]]]**

Syntax Definitions

fips	Displays FIP snooping sessions on FCoE ports.
npiv-proxy	Displays N_Port proxy (NPIV) sessions between ENode and FC switch.
r-npiv	Displays F_Port proxy (R- NPIV) sessions between the HBA and the gateway switch.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1).
vlan_id	An existing FCoE VLAN ID. The valid ID range is 2–4094.
agg_id	The link aggregate ID number.
tunnel_id	Displays E2E tunnel sessions between two E_Ports on different FC switches. Optionally enter a tunnel ID to display information for a specific tunnel.

Defaults

By default, all FCoE sessions are displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **port** or **linkagg** parameter to display sessions for a specific FCoE port or link aggregate ID.
- Use the **vlan** parameter to display the sessions for a specific FCoE VLAN ID.
- The output displays for this command include FIP snooping, N_Port proxy (NPIV), F_Port proxy (reverse-NPIV), and E2E tunnel sessions. However, the N_Port proxy, F_Port proxy, and E2E tunnel sessions are only displayed on an OmniSwitch 6900 that is configured as an FCoE/FC gateway (see Chapter 43, “FCoE/FC Gateway Commands” for more information.

Examples

```
-> show fcoe sessions
Total FIP Snooping Sessions: 2
PORT   ENODE MAC        VN_PORT MAC          FCF MAC           VLAN   STATUS
----+-----------------+-----------------+-------------------+----+---------
1/1  00:00:00:11:22:33  0E:FC:00:00:00:05  00:AA:BB:00:00:05    100  SUCCESS
1/1  00:00:00:11:22:33  00:00:00:00:00:00  00:AA:BB:00:00:05    100  PENDING

Total NPIV Sessions: 1
IN-PORT VLAN     ENODE_MAC       VN_PORT_MAC         FCF MAC       STATUS  OUT-PORT
-------+----+-----------------+-----------------+-----------------+-------+--------
  1/1   100  00:00:00:11:23:34 0E:FC:00:00:00:00 00:AA:00:01:03:01 PENDING    2/1

Total R-NPIV Sessions: 2
IN-PORT VLAN VSAN   FCID     VN_PORT_MAC         FCF MAC       STATUS    OUT-PORT
-------+----+----+--------+-----------------+-----------------+---------+--------
  2/2   400   400 01:02:02 0E:FC:00:01:02:02 00:AA:00:01:02:02  SUCCESS    1/2
  2/3    -     20 01:03:01        -                 -           SUCCESS    2/1

Total E-TUNNEL sessions: 3
TUNNEL-ID   PORT1   PORT2   VLAN    PAIR MODE     FCF MAC         STATUS
----------+--------+------+-------+-----------+-----------------+---------
    1        2/12    2/12    -      TE to TE        -             SUCCESS
   10        2/3     1/4    10      TE to VE   00:E0:B1:71:23:12  SUCCESS
   20        2/4     1/5    300     TE to VE   00:E0:B1:71:23:10  SUCCESS

-> show fcoe sessions fips
Total FIP Snooping Sessions: 2
PORT   ENODE MAC        VN_PORT MAC          FCF MAC           VLAN   STATUS
----+-----------------+-----------------+-------------------+----+---------
1/1  00:00:00:11:22:33  0E:FC:00:00:00:05  00:AA:BB:00:00:05    100  SUCCESS
1/1  00:00:00:11:22:33  00:00:00:00:00:00  00:AA:BB:00:00:05    100  PENDING

-> show fcoe sessions npiv-proxy
Total NPIV Sessions: 1
IN-PORT VLAN     ENODE_MAC       VN_PORT_MAC         FCF MAC       STATUS  OUT-PORT
-------+----+-----------------+-----------------+-----------------+-------+--------
  1/1   100  00:00:00:11:23:34 0E:FC:00:00:00:00 00:AA:00:01:03:01 PENDING    2/1

-> show fcoe sessions r-npiv
Total R-NPIV Sessions: 2
IN-PORT VLAN VSAN   FCID     VN_PORT_MAC         FCF MAC       STATUS    OUT-PORT
-------+----+----+--------+-----------------+-----------------+---------+--------
  2/2   400   400 01:02:02 0E:FC:00:01:02:02 00:AA:00:01:02:02  SUCCESS    1/2
  2/3    -     20 01:03:01        -                 -           SUCCESS    2/1

-> show fcoe sessions e-tunnel
Total E-TUNNEL sessions: 3
TUNNEL-ID   PORT1   PORT2   VLAN    PAIR MODE     FCF MAC         STATUS
----------+--------+------+-------+-----------+-----------------+---------
    1        2/12    2/12    -      TE to TE        -             SUCCESS
   10        2/3     1/4    10      TE to VE   00:E0:B1:71:23:12  SUCCESS
   20        2/4     1/5    300     TE to VE   00:E0:B1:71:23:10  SUCCESS
```

```
-> show fcoe sessions e-tunnel 10
Total E-TUNNEL sessions: 3
TUNNEL-ID   PORT1   PORT2   VLAN    PAIR MODE     FCF MAC         STATUS
----------+--------+------+-------+-----------+-----------------+---------
   10        2/3     1/4    10      TE to VE   00:E0:B1:71:23:12  SUCCESS

-> show fcoe sessions vlan 10
Total FIP Snooping Sessions              : 2
Total FIP Snooping Sessions on VLAN 10   : 1
PORT   ENODE MAC        VN_PORT MAC          FCF MAC           VLAN   STATUS
----+-----------------+-----------------+--------------------+----+---------
1/1  00:00:00:11:22:33  0E:FC:00:00:00:05  00:AA:BB:00:00:05     10  SUCCESS

Total NPIV Sessions              : 3
Total NPIV Sessions on VLAN 10   : 1
IN-PORT VLAN     ENODE_MAC       VN_PORT_MAC         FCF MAC       STATUS  OUT-PORT
-------+----+----------------+----------------+----------------+-------+--------
  1/1    10  00:00:00:11:23:34 0E:FC:00:00:00:00 00:AA:00:01:03:01 PENDING    2/1

Total R-NPIV Sessions              : 3
Total R-NPIV Sessions on VLAN 10   : 1
IN-PORT VLAN VSAN   FCID     VN_PORT_MAC         FCF MAC       STATUS    OUT-PORT
-------+----+----+--------+----------------+----------------+---------+--------
  2/2    10   400 01:02:02 0E:FC:00:01:02:02 00:AA:00:01:02:02  SUCCESS    1/2

Total E-TUNNEL Sessions            : 3
Total E-TUNNEL Sessions on VLAN 10 : 1
TUNNEL-ID   PORT1   PORT2   VLAN    PAIR MODE     FCF MAC         STATUS
----------+--------+------+-------+-----------+-----------------+---------
   10        2/3     1/4    10      TE to VE   00:E0:B1:71:23:12  SUCCESS

-> show fcoe sessions fips port 1/1
Total FIP Snooping Sessions               : 4
Total FIP Snooping Sessions on Port 1/1   : 2
PORT   ENODE MAC        VN_PORT MAC          FCF MAC           VLAN   STATUS
----+-----------------+-----------------+--------------------+----+---------
1/1  00:00:00:11:22:33  0E:FC:00:00:00:05  00:AA:BB:00:00:05    100  SUCCESS
1/1  00:00:00:11:22:33  00:00:00:00:00:00  00:AA:BB:00:00:05    100  PENDING

-> show fcoe sessions npiv linkagg 1
Total NPIV Sessions                : 3
Total NPIV Sessions on Linkagg 1   : 1

IN-PORT VLAN     ENODE_MAC       VN_PORT_MAC         FCF MAC       STATUS  OUT-PORT
-------+----+----------------+----------------+----------------+-------+--------
  0/10  100  00:00:00:11:23:34 0E:FC:00:00:00:00 00:AA:00:01:03:01 PENDING    2/1
```

output definitions

PORT	The FCoE port or link aggregate ID for a FIP snooping session. A “0” slot number indicates that the FCoE interface is a link aggregate. Configured through the **fcoe role** command.
ENODE MAC	The MAC address of the ENode for this session.
VN_PORT MAC	The MAC address of the virtual node (VN) port for this session.
FCF MAC	The MAC address of the FCoE Forwarder (FCF) for this session.

output definitions

VLAN	The FCoE VLAN used for this session. Configured through the **fcoe vlan** command.
STATUS	The operational status of this session.
IN-PORT	The FCoE port or link aggregate ID for an N_Port proxy (NPIV) or F_Port proxy (R-NPIV) session. Configured through the **fcoe role** command.
OUT-PORT	The FC port for an N_Port proxy (NPIV) or F_Port proxy (R-NPIV) session. Configured through the **fibre-channel port mode** command.
VSAN	The VSAN ID mapped to the FCoE VLAN ID for an F_Port proxy (R-NPIV) session. Configured through the **fibre-channel vsan** command.
FCID	The FC port ID (also referred to as N_Port ID) received after successful login for an F_Port proxy (R-NPIV) session.
TUNNEL-ID	The E2E tunnel ID associated with the session. Configured through the **fcoe e-tunnel** command.
PORT1, PORT2	The FCoE port (in VE_Port role) and/or FC port (in TE_Port mode) for this session. The FCoE port rule is configured through the **fcoe role** command. The FC port mode is configured through the **fibre-channel port mode** command.
PAIR MODE	The type of E2E tunnel (**TE to VE** or **TE to TE**).

Release History

Release 7.3.2; command introduced.
Release 7.3.3; fields added to display NPIV, reverse-NPIV, and E2E tunnel sessions.

Related Commands

show fcoe	Displays the global FCoE and FIP snooping configuration for the switch.
show fcoe ports	Displays the FCoE port configuration for the switch.
show fibre-channel port	Displays the FC port configuration for the switch.

MIB Objects

AlaFipsSessionTable

- alaFipsSessionEnodeMAC
- alaFipsSessionVNMAC
- alaFipsSessionVlanId
- alaFipsSessionIfIndex
- alaFipsSessionFCFMAC

AlaFipsNpivSessionTable

- alaFipsNpivSessionEnodeMAC
- alaFipsNpivSessionVNMAC
- alaFipsNpivSessionVlanId
- alaFipsNpivSessionInIfIndex
- alaFipsNpivSessionOutIfIndex
- alaFipsNpivSessionFCFMAC

AlaFipsRnpivSessionTable

- alaFipsRnpivSessionVNMAC
- alaFipsRnpivSessionVlanId
- alaFipsRnpivSessionInIfIndex
- alaFipsRnpivSessionOutIfIndex
- alaFipsRnpivSessionFCFMAC
- alaFipsRnpivSessionStatus
- alaFipsRnpivSessionVsanId
- alaFipsRnpivSessionFcid

AlaFipsEtunnelSessionTable

- alaFipsEtunnelSessionTunnelId
- alaFipsEtunnelSessionVlanId
- alaFipsEtunnelSessionInIfIndex
- alaFipsEtunnelSessionOutIfIndex
- alaFipsEtunnelSessionFCFMAC
- alaFipsEtunnelSessionStatus
- alaFipsEtunnelSessionPairMode

show fcoe enode

Displays FCoE Node (ENode) information for FIP Snooping sessions associated with the switch.

show fcoe enode [*mac_address***]**

Syntax Definitions

mac_address	Enter an ENode MAC Address (for example, 00:00:39:59:f1:0c).

Defaults

By default, information is displayed for all ENodes associated with the switch.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Specify an ENode MAC address to display more detailed information about a specific ENode.

Examples

```
-> show fcoe enode
Port   Enode MAC         VLAN       Sessions
----+------------------+-----+------------
1/1  00:10:00:00:00:02    100             2
2/1  00:00:a0:bb:00:01    200             1

->show fcoe enode 00:10:00:00:00:02
Enode MAC: 00:10:00:00:00:02   Port : 1/1

    VN-Port-MAC          FCF-MAC       Vlan     Login time
------------------+------------------+----+-------------------------
 0E:FC:00:00:00:15   00:AE:00:00:00:01  100  Thu Feb 14 07:22:54 2013
 0E:FC:00:00:00:09   0E:AE:00:00:00:01  200  Thu Feb 14 07:12:22 2013
```

output definitions

Port	The slot/port or link aggregate ID of the FCoE interface that is connected to the FCoE Node (ENode). A “0” slot number indicates that the FCoE interface is a link aggregate.
Enode MAC	The MAC address of the ENode connected to the FCoE interface.
VLAN	The FCoE VLAN ID.
Sessions	The number of sessions associated with the ENode MAC.
VN-Port-MAC	The MAC address of the virtual node port (VN_port) for this session.
FCF-MAC	The MAC address of the FCoE Forwarder (FCF).
Login time	The date and time the ENode logged into the FCoE fabric.

Release History

Release 7.3.2; command introduced.

Related Commands

show fcoe sessions	Displays FCoE FIP snooping session status and configuration for the switch.
show fcoe fcf	Displays FCoE Forwarder (FCF) information for the switch.

MIB Objects

```
alaFipsSessionTable
   alaFipsSessionEnodeMAC
   alaFipsSessionVNMAC
   alaFipsSessionVlanId
   alaFipsSessionIfIndex
   alaFipsSessionFCFMAC
   alaFipsSessionLoginTime
```

show fcoe fcf

Displays FCoE Forwarder (FCF) information for FIP Snooping sessions associated with the switch.

show fcoe fcf [*mac_address***]**

Syntax Definitions

mac_address	Enter an FCF Address (for example, 00:00:39:59:f1:0c).

Defaults

By default, information is displayed for all FCFs associated with the switch.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Specify an FCF MAC address with this command to display more detailed information for a specific FCF.

Examples

```
-> show fcoe fcf
       FCF-MAC         VLAN    Config     Sessions  A-bit   MaxFrmVer  Priority
--------------------+-------+----------+---------+-------+---------+----------
  E8:E7:32:3F:FD:F0    46       Npiv        4         1         0         0
  E8:E7:32:63:8B:B0    56       Dynamic     1         1         1         128
  E8:E7:32:94:68:17    4000     Dynamic     0         1         0         128
  E8:E7:32:94:68:E8    3000     Static      0         1         1         0
  E8:E7:32:94:68:EE    4000     Static      0         1         1         0

-> show fcoe fcf E8:E7:32:3F:FD:F0
FCF : E8:E7:32:3F:FD:F0

 VLAN      VN-Port-MAC
-------+-----------------
 46      0E:FC:00:01:00:03
 46      0E:FC:00:01:00:80
 46      0E:FC:00:01:00:82
 46      0E:FC:00:01:00:81
```

output definitions

FCF-MAC	The MAC address of the FCoE Forwarder (FCF).
VLAN	The FCoE VLAN ID.
Config	Whether the FCF MAC address was user-configured or learned through the FIP Snooping session for the given FCoE VLAN.
Sessions	The number of sessions associated with the FCF MAC for the given FCoE VLAN.
A-bit	Whether or not the available-for-login bit is set for this FCF.

output definitions

MaxFrmVer	Whether or not the maximum frame size was verified for this FCF.
VN-Port-MAC	The MAC address of the virtual node port (VN_Port) for this session. This address is comprised of the FCID that the FCF assigned to the port combined with the FC-MAP.

Release History

Release 7.3.2; command introduced.
Release 7.3.3; **A-bit** and **MaxFrmVer** fields added.

Related Commands

show fcoe sessions	Displays FCoE FIP snooping session status and configuration for the switch.
show fcoe enode	Displays FCoE Node (ENode) information for the switch.

MIB Objects

```
alaFipsFcfTable
   alaFipsFcfSessions
   alaFipsSessionFCFMAC
   alaFipsSessionVlanId
   alaFipsFcfConfigType
   alaFipsFcfAvailForLogin
   alaFipsFcfMaxFcoeFrmSizeVerified
```

show fcoe fc-map

Displays the Fibre Channel Mapped Address Prefix (FC-MAP) for each FCoE VLAN.

show fcoe fc-map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

When the FCoE address mode is set to Fabric-Provided MAC Address (FPMA), the FC-MAP value is the required upper 24 bits of a MAC address that is assigned to a Virtual N_Port (VN_Port).

Examples

```
-> show fcoe fc-map
  VLAN     FC-MAP
--------+-----------
     10   0E:FC:00
    100   0E:FC:22
    200   0E:FC:23
    300   0E:FC:23
```

Release History

Release 7.3.2; command introduced.

Related Commands

fcoe vlan	Configures an FCoE VLAN for the switch.
fcoe fc-map	Configures the FC-MAP for and FCoE VLAN.
show vlan	Displays the VLAN configuration for the switch.

MIB Objects

```
alaFipsVlanTable
   alaFipsVlanId
   alaFipsVlanFCMap
```

show fcoe discovery-advertisement

Displays the FIP discovery advertisement message parameter values for the specified FCoE VLAN.

show fcoe discovery-advertisement [vlan *vlan_id***[-***vlan_id2***]]**

Syntax Definitions

*vlan_id***[-***vlan_id2***]**	An existing FCoE VLAN ID. Use a hyphen to specify a range of FCoE VLAN IDs (10-25).

Defaults

By default, the discovery advertisement parameters are displayed for all FCoE VLANs.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the *vlan_id***[-***vlan_id2***]** parameter to display information for a specific FCoE VLAN or for a range of FCoE VLANs.

Examples

```
-> show fcoe discovery-advertisement
VLAN  A-Bit   FKA Pd Priority  UDS-Retries
----+--------+------+--------+--------------
46    ENABLE  8      128      3
56    ENABLE  8      128      3
76    ENABLE  8      128      3
3000  ENABLE  8      128      3
4000  ENABLE  8      128      3

-> show fcoe discovery-advertisement vlan 3000
  VLAN     A-Bit      FKA Period    Priority       UDS-Retries
---------+----------+------------+-----------+----------------
   3000    ENABLE        8           128            3
```

output definitions

VLAN	The FCoE VLAN ID. Configured through the **fcoe vlan** command**.**
A-Bit	The status of the available-for-login bit (Enabled or Disabled). When enabled, indicates the switch can accept fabric logins from ENodes.
FKA-PD	The discovery advertisement transmission interval, in seconds.
Priority	The priority value assigned to the switch (0 = highest priority, 255 = lowest priority.
UDS-Retries	The number of times a unicast discovery solicitation is transmitted after a port on which an FCF MAC was learned goes down.

Release History

Release 7.3.3; command introduced.

Related Commands

fcoe discovery-advertisement Configures FIP discovery advertisement parameter values.

MIB Objects

```
alaFipsDiscAdvtTable
   alaFipsDiscAdvtVlanId
   alaFipsDiscAdvtAbit,
   alaFipsDiscAdvtFkaAdvPeriod,
   alaFipsDiscAdvtPriority,
   alaFipsDiscAdvtUdsRetries,
   alaFipsDiscAdvtRowStatus
```

show fcoe statistics

Displays both ENode and FCF generated statistics for FCoE interfaces or specific VLANs.

show fcoe statistics [enode | fcf] {interface | vlan [*vlan_id***[***vlan_id2***] | port** *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

enode	Display statistics only for ENode traffic.
fcf	Display statistics only for FCF traffic.
interface	Display statistics for all FCoE interfaces (ports and link aggregates).
*vlan_id***[-***vlan_id2***]**	An existing FCoE VLAN ID. Use a hyphen to specify a range of FCoE VLAN IDs (10-25).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, FCF and ENode statistics are displayed for all FCoE interfaces and VLANs.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **vlan** parameter to display statistics for a specific FCoE VLAN ID.
- Use the **port** or **linkagg** parameters to display statistics for a specific FCoE port or link aggregate ID.
- The output displays for this command include FIP snooping, N_Port proxy (NPIV), and F_Port proxy (reverse-NPIV) statistics. However, the N_Port proxy and F_Port proxy statistics are only displayed on an OmniSwitch 6900 that is configured as an FCoE/FC gateway (see Chapter 43, “FCoE/FC Gateway Commands” for more information.

Examples

```
-> show fcoe statistics interface
Enode Statistics

Port     Sess   VL REQ   MDS    UDS     FLOGI    FDISC   LOGO     E KA    VN KA
-------+------+-------+-------+-------+--------+-------+-------+--------+--------
1/17         0       0       0       0        0       0       0        0        0

FCF Statistics
Port  Sess  VL RESP MDA  UDA  FLOGI_ACC FLOGI_RJT FDISC_ACC FDISC_RJT LOGO_ACC LOGO_RJT  CVL
-----+-----+-------+---+-----+---------+---------+---------+---------+--------+--------+-----
1/17      0       0   0 32997         0         0         0         0        0        0     0
```

```
NPIV Enode-Discovery Statistics

Packets Received:
   Port   Vlan Req     MDS       UDS
---------+---------+---------+---------
 1/17             0         0         0
Packets Sent:
   Port    Vlan Res    MDA       UDA
---------+---------+---------+---------
 1/17             0         0         0

NPIV Enode-Login Statistics

Packets Received:
   Port     FLOGI     FDISC      LOGO     E_KA      VN_KA
---------+---------+---------+---------+---------+---------
 1/17             0         0         0         0         0
Packets Sent:
   Port   FLOGI_ACC FDISC_ACC FLOGO_ACC FLOGI_RJT FDISC_RJT FLOGO_RJT    CVL
---------+---------+---------+---------+---------+---------+---------+---------
 1/17             0         0         0         0         0         0         0

R-NPIV FCF-Discovery Statistics

Packets Received:
   Port      MDA       UDA
---------+---------+---------
 1/17         32991         1
Packets Sent:
   Port      MDS       UDS
---------+---------+---------
 1/17             0         1

R-NPIV Node-Login Statistics

Packets Received:
   Port   FLOGI_ACC FDISC_ACC FLOGI_RJT FDISC_RJT   CVL
---------+---------+---------+---------+---------+---------
 1/17             2         0         0         0         0
Packets Sent:
   Port     FLOGI     FDISC     LOGO      VN-KA     E-KA
---------+---------+---------+---------+---------+---------
 1/17             2         0         1      2952     33191

-> show fcoe statistics enode interface
Enode Statistics

  Port     Sess      MDS      UDS     FLOGI    FDISC    LOGO        E KA         VN KA
--------+--------+--------+--------+--------+--------+--------+------------+------------
 1/2           0         0        0        0        0        0             0             0
 1/12          0         0        0        0        0        0             0             0

-> show fcoe statistics vlan
Enode Statistics

  VLAN     Sess      MDS     UDS     FLOGI     FDISC    LOGO       E KA       VN KA
--------+--------+--------+--------+--------+--------+--------+------------+------------
 200            0        0    33415        0        0        0             0             0

FCF Statistics
VLAN Sess MDA  UDA  FLOGI_ACC FLOGI_RJT FDISC_ACC FDISC_RJT LOGO_ACC LOGO_RJT CVL
----+----+----+----+---------+---------+---------+---------+--------+--------+-----
200    0    0    0         0         0         0         0        0        0     0
```

```
NPIV Enode-Discovery Statistics

Packets Received:
   Vlan    Vlan Req    MDS       UDS
---------+---------+---------+---------
 200              0         0         0
Packets Sent:
   Vlan   Vlan Res     MDA       UDA
---------+---------+---------+---------
 200              0         0         0

NPIV Enode-Login Statistics

Packets Received:
  Vlan    FLOGI     FDISC     LOGO      E_KA      VN_KA
-------+---------+---------+---------+---------+---------
 200            0         0         0         0         0
Packets Sent:
  Vlan  FLOGI_ACC FDISC_ACC FLOGO_ACC FLOGI_RJT FDISC_RJT FLOGO_RJT    CVL
-------+---------+---------+---------+---------+---------+---------+---------
 200            0         0         0       118         0         0         0

R-NPIV FCF-Discovery Statistics

Packets Received:
   Vlan      MDA       UDA
---------+---------+---------
 200          33409         1
Packets Sent:
   Vlan      MDS       UDS
---------+---------+---------
 200              0         1

R-NPIV Node-Login Statistics

Packets Received:
   Vlan   FLOGI_ACC FDISC_ACC FLOGI_RJT FDISC_RJT   CVL
---------+---------+---------+---------+---------+----------
 200              2         0         0         0         0
Packets Sent:
   Vlan     FLOGI     FDISC     LOGO      VN-KA     E-KA
---------+---------+---------+---------+---------+---------
 200              2         0         1      2990     33611

-> show fcoe statistics fcf vlan
FCF Statistics

VLAN Sess MDA  UDA  FLOGI_ACC FLOGI_RJT FDISC_ACC FDISC_RJT LOGO_ACC LOGO_RJT  CVL
----+----+----+----+---------+---------+---------+---------+--------+--------+-------
200    0    0    0         0         0         0         0        0        0      0
```

output definitions

Port	The slot/port or link aggregate ID of the FCoE interface. A “0” slot number indicates that the FCoE interface is a link aggregate.
Sess	The number of FIP Snooping sessions.
MDS	The number of Multicast Discovery Solicitation packets.
UDS	The number of Unicast Discovery Solicitation packets.
FLOGI	The number of Fabric Login packets.
FDISC	The number of Fabric Discovery packets.

output definitions

LOGO	The number of Fabric Logout packets.
E KA	The number of ENode keep-alive packets.
VN KA	The number of VN_Port keep-alive packets
VLAN	The FCoE VLAN ID.
MDA	The number of Multicast Discovery Advertisement packets.
UDA	The number of Unicast Discovery Advertisement packets.
FLOGI_ACC	The number of Fabric Login Accept packets.
FLOGI_RJT	The number of Fabric Login Reject packets.
FDISC_ACC	The number of Fabric Discovery Accept packets.
FDISC_RJT	The number of Fabric Discover Reject packets.
LOGO_ACC	The number of Fabric Logout Accept packets.
LOGO_RJT	The number of Fabric Logout Reject packets.
CVL	The number of Clear Virtual Link packets.

Release History

Release 7.3.2; command introduced.
Release 7.3.3; N_Port proxy and F_Port proxy statistics displayed only on an OmniSwitch 6900.

Related Commands

clear fcoe statistics	Clears ENode and FCF statistics.

MIB Objects

```
alaFipsIntfEnodeStatsTable
alaFipsIntfFcfStatsTable
alaFipsVlanEnodeStatsTable
alaFipsVlanFcfStatsTable
```

clear fcoe statistics

Clears ENode and FCF generated statistics on FCoE interfaces or specific VLANs.

clear fcoe statistics [enode | fcf] [interface | vlan [*vlan_id***[***vlan_id2***] | port** *chassis/slot/port***[-***port2***]** | **linkagg** *agg_id***[-***agg_id2***]]**

Syntax Definitions

enode	Clears statistics only for ENode traffic.
fcf	Clears statistics only for FCF traffic.
interface	Clears statistics on all FCoE interfaces (ports and link aggregates).
*vlan_id***[***vlan_id2***]**	An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VLAN IDs (100-150).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, statistics are cleared for all FCoE interfaces and VLANs.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **port** or **linkagg** parameters to clear the statistics for a specific FCoE port or link aggregate ID.
- Use the **vlan** parameter to clear the statistics for a specific FCoE VLAN ID.

Examples

```
->clear fcoe statistics

->clear fcoe statistics interface

->clear fcoe statistics vlan
->clear fcoe statistics vlan 2
->clear fcoe statistics vlan 2-3

->clear fcoe statistics port 1/2
->clear fcoe statistics port 1/2-3
->clear fcoe statistics port 1/1/2
->clear fcoe statistics port 1/1/2-3

->clear fcoe statistics linkagg 2
->clear fcoe statistics linkagg 2-6
```

```
->clear fcoe statistics enode interface

->clear fcoe statistics enode vlan
->clear fcoe statistics enode vlan 2
->clear fcoe statistics enode vlan 2-3

->clear fcoe statistics enode port 1/2
->clear fcoe statistics enode port 1/2-3
->clear fcoe statistics enode port 1/1/2
->clear fcoe statistics enode port 1/1/2-3

->clear fcoe statistics enode linkagg 2
->clear fcoe statistics enode linkagg 2-6

->clear fcoe statistics fcf interface
->clear fcoe statistics fcf vlan
->clear fcoe statistics fcf vlan 2
->clear fcoe statistics fcf vlan 2-3

->clear fcoe statistics fcf port 1/2
->clear fcoe statistics fcf port 1/2-3
->clear fcoe statistics fcf port 1/1/2
->clear fcoe statistics fcf port 1/1/2-3

->clear fcoe statistics fcf linkagg 2
->clear fcoe statistics fcf linkagg 2-6
```

Release History

Release 7.3.2; command introduced.

Related Commands

show fcoe statistics	Displays ENode and FCF statistics for FCoE interfaces and VLANs.

MIB Objects

```
alaFipsConfig
   alaFipsConfigStatsClear
alaFipsIntfTable
   alaFipsIntfStatsClear
alaFipsVlanTable
   alaFipsVlanStatsClear
```

43 FCoE/FC Gateway Commands

The OmniSwitch implementation of FCoE/FC gateway functionality allows the switch to transparently connect FCoE and FC nodes with an FC SAN across an FCoE (lossless Ethernet) network. To provide this type of connectivity, an OmniSwitch FCoE/FC gateway supports the following three modes of operation that are used to converge FC over Ethernet and FC-to-FC over Ethernet:

- **N_Port Proxy mode**—allows ENodes in an FCoE network and FC switches in an FC SAN to communicate with each other. To an ENode the OmniSwitch gateway emulates an FCoE forwarder; to an FC switch the OmniSwitch gateway emulates an N_Port ID Virtualization (NPIV) host.
- **F_Port Proxy mode**—allows FC nodes to connect with FC switches and FCFs across an FCoE network. The OmniSwitch gateway forwards login requests from an FC node (N_Port on a server or storage with an HBA) across Ethernet via an FCoE VLAN to an NPIV node or FCF. This mode is sometimes referred to as reverse-NPIV proxy (R-NPIV).
- **E_Port Proxy mode**—allows FC switches to set up inter-switch link trunking between FC fabrics over an FCoE network. The OmniSwitch gateway provides an E_Port to E_Port (E2E) tunneling function that emulates a point-to-point FC link between E_Ports on native FC switches.

The OmniSwitch FCoE/FC gateway sits at the entry point of an FC fabric, which is required to handle the login process for ENodes and FC nodes accessing the fabric through the gateway switch.

OmniSwitch FCoE/FC gateway operations are not automatically activated for the switch; there is no single command to enable or disable gateway functionality. Instead, the configuration of the following software components enables one or more of the supported gateway operations:

- **FIP snooping**—FCoE/FC gateway functionality requires an active FIP snooping configuration. FIP Snooping ensures the security of an FCoE network.
- **Virtual Storage Area Network (VSAN)**—an FC port is assigned to a VSAN to create an NP_Port or F_Port connection to an FC switch or node in that VSAN. Not required for E2E Tunnel configuration.
- **VSAN-to-FCoE VLAN mapping**—identifies the FCoE/FC gateway fabric for the ENode or FC node login process via the FCoE VLAN. Not required for E_Port proxy (E2E Tunnel) configuration.
- **FC port mode**—the operational mode of the FC port determines the type of gateway functionality provided on that port. There are three modes supported: N_Port proxy, F_Port proxy, and E_Port proxy.
- **FCoE port role**—an FCoE port serves as an E2E tunnel endpoint in an FCoE network only when the port is configured as a virtual E_Port (VE_Port). The role of other FCoE ports is configured based on the FIP snooping configuration for the gateway switch.

This chapter and the Chapter 42, “FIP Snooping Commands,” describe the command line interface (CLI) commands used to configure these components.

MIB information for the FCoE/FC gateway commands is as follows:

Filename: ALCATEL-IND1-FIPS-MIB.mib
Module: alcatelIND1FipsMIB

The acronyms used in this chapter are defined here:

CNA	Converged Network Adapter
CVL	Clear Virtual Link
E2E	E_Port-to-E_Port Tunnel
ELP	Exchange Link Parameters
ENode	FCoE Node
E_Port	Expansion Port
F_Port	Fabric Port
FC	Fibre Channel
FCF	FCoE Forwarder
FDISC	Fabric Discovery
FCID	Fabric Port ID (same as N_Port ID).
FCoE	Fibre Channel over Ethernet
FIP	FCoE Initialization Protocol
FLOGI	Fabric Login
FLOGO	Fabric Logout
HBA	Host Bus Adapter
ISL	Inter-switch Link
NPIV	N_Port ID Virtualization
N_Port	Node Port
NP_Port	Proxy Node Port
TE_Port	Tunnel Expansion Port
VE_Port	Virtual E_Port
VF_Port	Virtual F_Port
VN_Port	Virtual N_Port
VSAN	Virtual Storage Area Network
WWNN	World Wide Node Name
WWPN	World Wide Port Name

The FCoE/FC gateway commands are listed here:

Configuration commands	**fibre-channel vsan** **fibre-channel port mode** **fibre-channel vsan members** **fcoe vsan-map** **fibre-channel npiv-proxy load-balance** **fibre-channel npiv-proxy load-balance static** **fcoe e-tunnel**
Show commands	**show fibre-channel vsan** **show fibre-channel vsan members** **show fibre-channel port** **show fcoe vsan-map** **show fibre-channel sessions** **show fibre-channel node** **show fcoe e-tunnel** **show fibre-channel** **show fibre-channel npiv-proxy load-balance**
Statistics commands	**show fibre-channel statistics** **show fcoe statistics npiv-proxy** **show fcoe statistics r-npiv** **show fcoe statistics e-tunnel**
Clear commands	**clear fibre-channel statistics** **clear fibre-channel sessions** **clear fcoe statistics npiv** **clear fcoe statistics r-npiv** **clear fcoe statistics e-tunnel** **clear fcoe sessions**

fibre-channel vsan

Configures an OmniSwitch VSAN with the specified VSAN ID and an optional description. This type of VSAN is used to segment OmniSwitch Fibre Channel ports into a virtual FCoE/FC gateway fabric.

Note. The VSAN created with this command only applies to the local switch configuration. There is no correlation between an OmniSwitch VSAN and a VSAN created within a native FC SAN.

fibre-channel vsan {*vsan_id***[-***vsan_id2***]} [admin-state {enable | disable}] [name** *description***]**

no fibre-channel vsan {*vsan_id***[-***vsan_id2***]}**

Syntax Definitions

*vsan_id***[-***vsan_id2***]**	A numeric value that will uniquely identify the VSAN. Use a hyphen to specify a range of VSAN IDs (for example, 100-105). The valid range is 2–4094).
enable	Enable the VSAN administrative status.
disable	Disable the VSAN administrative status.
description	An alphanumeric string. Optional name description for the VSAN ID.

Defaults

By default, VSAN 1 is created on the switch and all unassigned FC ports are assigned to VSAN 1.

parameter	default
enable | disable	**enable**
name *description*	**VSAN ID**

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to delete a VSAN from the configuration.
- When a VSAN is administratively disabled, all sessions established over that VSAN are cleared and the switch stops sending periodic FIP multicast discovery advertisement messages for the corresponding FCoE VLAN.
- The description can be any alphanumeric string. Enclose the description in double quotes if it contains more than one word with space in between.
- Only FC switch ports can be assigned to a VSAN.
- Assigning multiple FC ports to the same VSAN is allowed, but an FC port can only belong to one VSAN.

- Configuring N_Port and F_Port proxy functionality requires mapping a VSAN to an FCoE VLAN. Note that only one VSAN is mapped to one FCoE VLAN (one-to-one) at any given time. This mapping defines a single traffic path through the gateway switch.
- If an FCoE VLAN is not mapped to a VSAN, then the FCoE VLAN participates only in the FIP snooping process.

Examples

```
-> fibre-channel vsan 200 name “Fabric A”
-> fibre-channel vsan 100-105 admin-state disable
-> no fibre-channel vsan 200
```

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel vsan members	Assigns FC switch ports to a VSAN.
fcoe vsan-map	Maps a VSAN to an FCoE VLAN.
show fibre-channel vsan	Displays the VSAN configuration for the switch.
show fcoe vsan-map	Displays the VSAN-VLAN mapping configuration for the switch.
show fibre-channel vsan members	Displays FC port assignments for each VSAN.

MIB Objects

```
alaFcVsanTable
   alaFcVsanNumber
   alaFcVsanDescription,
   alaFcVsanAdmStatus
   alaFcVsanOperStatus
```

fibre-channel port mode

Configures the port type and operational mode for an eligible FC port. The port type is only set to Fibre Channel and the specified operational mode determines the type of gateway functionality provided on that port. There are three modes supported: N_Port proxy, F_Port proxy, and E_Port proxy.

fibre-channel port *chassis/slot/port***[**-*port2***] mode {np | f | te} [bb-sc-n** *buffer_num***]**

no fibre-channel port *chassis/slot/port***[**-*port2***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8). Only ports on an OmniSwitch 6900 OS-XNI-U12E module with an SFP-FC-SR transceiver are eligible for this command.
np	Activates N_Port proxy functionality on the port. In this mode the port serves as a proxy node port (NP_Port) that aggregates N_Port transactions between FCoE devices and FC switches.
f	Activates F_Port proxy functionality on the port. In this mode the port operates as a fabric port (F_Port), which connects to an N_Port in a point-to-point link between FC devices.
te	Activates E_Port functionality on the port. In this mode, the port operates as a tunnel expansion port (TE_Port) that connects to an E_Port on an FC switch. TE_Ports allow E_Ports to connect across an FCoE network as part of an inter-switch link (ISL) tunnel that is used to expand the native FC fabric over Ethernet.
buffer_num	The buffer-to-buffer state change (BB_SC) number. FC ports exchange BB_SC primitives after 2^BB_SC_N frames. These primitives are used to recalculate buffer credits as part of a buffer-to-buffer flow control function between FC switch connections. The valid range is 0–15.

Defaults

By default, no operational mode is configured for the FC ports and the port type is set to Ethernet.

parameter	default
bb-sc-n *buffer_num*	**0**

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the operational mode configuration from the FC port. The port type reverts back to Ethernet.
- To change the FC mode for the port, use the **no** form of this command to remove the current mode configuration then configure the FC mode again for the same port.

- Changing the **bb-sc-n** parameter value can be changed at any time (removing the FC mode configuration is not required to change this parameter value).
- Make sure the **bb-sc-n** parameter value is the same on both ends of the connection between the OmniSwitch FCoE/FC gateway and an FC switch. If the value is different on each end of the connection then the greater value is used. However, if this value is set to zero for one of the ports on the connection, then the buffer-to-buffer state change function is disabled.
- FC ports do not participate in Ethernet features, such as a link aggregates, a virtual fabric links (VFLs) in virtual chassis (VC) configurations, standard VLANs, or FCoE VLANs.
- To ensure end-to-end lossless connectivity through the gateway switch, assign a PAUSE-enabled DCB profile to each FC port. For more information, see Chapter 5, “Configuring an FCoE Gateway”, in the *OmniSwitch AOS Release 8 Data Center Switching Guide*.

Examples

```
-> fibre-channel port 2/1 mode np
-> fibre-channel port 2/3 mode f
-> fibre-channel port 2/5 mode te
-> no fibre-channel port 2/5
```

To change the FC port mode:

```
-> no fibre-channel port 2/1
-> fibre-channel port 2/1 f
```

To change the **bb-sc-n** parameter value:

```
-> fibre-channel port 2/1 bb-sc-n 3
```

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel vsan members	Assigns FC ports to VSANs.
show fibre-channel port	Displays the FC port configuration for the switch.

MIB Objects

```
alaFcIntfTable
   alaFcIntfIfIndex
   alaFcIntfMode
   alaFcIntfBbScN
   alaFcIntfBbCredit
   alaFcIntfBbRxDataField
   alaFcIntfClassOfService
   alaFcIntfRowStatus
```

fibre-channel vsan members

Configures the VSAN assignment for the specified FC port.

fibre-channel vsan *vsan_id* **members port** *chassis/slot/port***[**-*port2***]**

no fibre-channel vsan *vsan_id* **members port** *chassis/slot/port***[**-*port2***]**

Syntax Definitions

vsan_id	An existing VSAN ID number.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

Defaults

By default, all FC ports are assigned to VSAN 1.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the association between the specified FC port and VSAN.
- When an NP_Port is removed from a VSAN, a FIP CVL is generated for all the VN_Ports that are logged in through that NP_Port and an FC LOGO is sent on the FC port. An FC LOGO is also sent for any R-NPIV sessions that exist when the CVL is generated.
- When an F_Port (used for R-NPIV) is removed from a VSAN, then FC LOGO is sent to the host and also to the FCF.
- When an FC port is moved from VSAN 1 to another VSAN, traffic loss will occur for all existing sessions. Moving FC ports between other VSANs (for example, between VSAN 2 and 3) is not allowed.
- Multiple FC ports can belong to the same VSAN, but an FC port can belong to only one VSAN. In other words, it is not possible to tag FC ports with multiple VSANs.
- When a VSAN is mapped to an FCoE VLAN and an active FC port is assigned to that VSAN, the FC mode configured for that port determines the FCoE/FC gateway functionality provided. For example, if the FC port mode is set to operate as:
  - an NP_Port, then NPIV proxy functionality is automatically enabled.
  - an F_Port, then the R-NPIV functionality is automatically enabled.
  - a TE_Port and an FCoE port is set to operate as a virtual E_Port (VE_Port), then E2E tunneling functionality is automatically enabled.

- When more than one NP_Port is associated with the same VSAN, the OmniSwitch will load balance ENode FLOGI requests across the NP_Ports for that VSAN. By default, the NP_Port with the lowest number of logins provided is selected. If all the NP_Ports have the same number of logins provided, then the switch will select a port using a round robin algorithm.

Examples

```
-> fibre-channel vsan 10 members port 2/1
-> fibre-channel vsan 10 members port 2/1-3
-> no fibre-channel vsan 10 members port 2/1-3
```

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel vsan	Creates an FC VSAN.
fibre-channel port mode	Configures the operational mode for the FC port.
fibre-channel npiv-proxy load-balance	Configures the load balancing method applied when more than one FC port is assigned to the same VSAN.
show fibre-channel vsan	Displays the VSAN configuration for the switch.
show fibre-channel vsan members	Displays the VSAN port assignments.

MIB Objects

```
alaFcVfpaTable
   alaFcVfpaVsanNumber
   alaFcVfpaIfIndex
   alaFcVfpaRowStatus
```

fcoe vsan-map

Maps an FC VSAN to an FCoE VLAN. This mapping is required to activate the processing of specific FCoE ENode traffic traveling to and from the designated virtual FC fabric through the FCoE/FC gateway OmniSwitch.

fcoe vsan-map vsan *vsan_id* **vlan** *vlan_id*

no fcoe vsan-map vsan *vsan_id* **vlan** *vlan_id*

Syntax Definitions

vsan_id	An existing VSAN ID number.
vlan_id	An existing FCoE VLAN ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the VSAN-to-FCoE VLAN mapping.
- When a mapping is removed, all sessions associated with the FCoE VLAN are cleared.
- Only one VSAN is mapped to one FCoE VLAN.
- The FCoE/FC gateway does not participate in FCoE discovery mechanisms for FCoE VLANs not mapped to a VSAN.
- If an FCoE VLAN is not mapped to a VSAN, then only FIP snooping functionality is applied to that VLAN.

Examples

```
-> fcoe vsan-map vsan 10 vlan 100
-> no fcoe vsan-map vsan 10 vlan 100
```

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel vsan	Configures a VSAN for the switch.
fcoe vlan	Configures an FCoE VLAN for the switch.
show fcoe vsan-map	Displays the VSAN-VLAN mapping configuration.

MIB Objects

```
alaFipsVsanVlanMapTable
   alaFipsVsanVlanMapVsanNumber
   alaFipsVsanVlanMapVlanNumber
   alaFipsVsanVlanMapRowStatus
```

fibre-channel npiv-proxy load-balance

Configures the dynamic load balancing method that is applied to ENode FLOGI requests when more than one FC port is associated with the same VSAN. Load balancing is not applied to FDISC requests.

fibre-channel npiv-proxy load-balance static {default | dynamic-reorder | enode-based}

Syntax Definitions

default	Selects the default load balancing method.
dynamic-reorder	Ensures that all sessions are load balanced evenly at any given time.
enode-based	Selects the FC for the new session based on the ENode MAC address.

Defaults

By default, the FC port with the lowest number of logins provided is selected for new FLOGI requests. If all the ports have the same number of logins provided, then the switch will select a port using a round robin algorithm.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The load balancing method is globally applied to the switch, and only one method is applied at a time.
- Using the dynamic reorder load balancing method may trigger the tearing down of some sessions, so that upon re-login the ENode FLOGI is processed on a different NP_Port in the same VSAN. For example, when a new FC NP_Port is added to the VSAN, some of the sessions are torn down and logged in again on the newly added port to distribute sessions across all ports in the VSAN.
- When the ENode-based load balancing method is used, each NP_Port in the VSAN will send a multicast discovery advertisement to all ENodes in the mapped FCoE VLAN. The FCF MAC address in the discovery advertisement is the MAC address of the FC port. The ENode then decides which FCF (NP_Port) to use for the login.
- The default and ENode-based load balancing methods do not disturb existing sessions.
- The load balancing method is *not* applied to statically mapped FCoE and FC ports.

Examples

```
-> fibre-channel npiv-proxy load-balance dynamic-reorder
-> fibre-channel npiv-proxy load-balance enode-based
-> fibre-channel npiv-proxy load-balance default
```

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel npiv-proxy load-balance static	Configures a static mapping between an FCoE port and an FC NP_Port. Load balancing does not apply to statically mapped ports.
show fibre-channel	Displays the global load balancing method applied to NP_Ports.

MIB Objects

```
alaFcInfo
   alaFcConfigNpivLoadBalance
```

fibre-channel npiv-proxy load-balance static

Configures a static port association between an FCoE port and an FC NP_Port to ensure that FC sessions on the specified FCoE port are mapped to the specified NP_Port.

fibre-channel npiv-proxy load-balance static {port *chassis/slot/port* | **linkagg** *agg_id***} fc-port** *chassis/slot/port*

no fibre-channel npiv-proxy load-balance static {port *chassis/slot/port* | **linkagg** *agg_id***} fc-port** *chassis/slot/port*

Syntax Definitions

chassis	The chassis identifier.
port *slot/port*	The slot and port number (3/1) of an FCoE port.
agg_id	The link aggregate ID number.
fc-port *slot/port*	The slot and port number (3/1) of an FC port.

Defaults

By default, there are no static FCoE-to-FC port associations. The dynamic load balancing method is applied to the FC NP_ports.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the static association between the FCoE port and the FC port. When this association is removed, the dynamic load balancing method is applied.
- Use caution when configuring static FCoE-to-FC port assignments. Static assignments exempt both the FCoE port and the FC NP_Port from dynamic load balancing of sessions when multiple FC ports belong to the same VSAN.

Examples

```
-> fibre-channel npiv-proxy load-balance static port 1/1 fc-port 2/1
-> no fibre-channel npiv-proxy load-balance static port 1/1 fc-port 2/1

-> fibre-channel npiv-proxy load-balance static linkagg 10 fc-port 2/1
-> no fibre-channel npiv-proxy load-balance static linkagg 10 fc-port 2/1
```

Release History

Release 7.3.3; command introduced.

Related Commands

show fibre-channel npiv-proxy load-balance	Displays the static FCoE port/FC NP_Port mapping and FC port session counts.

MIB Objects

```
alaFcNpivStaticLoadBalanceTable
   alaFcNpivStaticLoadBalanceRowStatus
   alaFcNpivStaticLoadBalanceEtherIfIndex
   alaFcNpivStaticLoadBalanceFibreIfIndex
```

fcoe e-tunnel

Configures an E2E tunnel identifier and associates the identifier with tunnel endpoints and an FCoE VLAN. An E2E tunnel allows FC switches to set up ISLs between fabrics over an FCoE network.

fcoe e-tunnel *tunnel_id* **{fc-port1** *chassis/slot/port***} {fc-port2** *chassis/slot/port* | **vlan** *vlan_id***}**

no fcoe e-tunnel *tunnel_id*

Syntax Definitions

tunnel_id	A unique ID number to assign to this tunnel session.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1) of an FC tunnel edge (TE) port.
vlan_id	An existing FCoE VLAN ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the tunnel configuration.
- An OmniSwitch FC port is configured as a tunnel E_Port (TE_Port) and connects to an E_Port on an FC switch. TE_Ports can carry traffic from multiple VSANs. This command is used to associate the TE port with an FCoE VLAN or with another TE port on the same switch.
- An OmniSwitch FCoE port is configured as a virtual expansion port (VE_Port) on the FCoE network side. The VE port is associated with an FCoE VLAN by tagging the VE port with the FCoE VLAN ID.
- This command does not establish a connection. Once the required tunnel components are configured, successful exchange of exchange link parameters (ELP) between a TE_Port and a VE_Port or between two TE_Ports will establish the tunnel session.
- To create a tunnel connection between two FC switches across the FCoE network requires the following steps:
  - Configure the FCoE port that will connect to the FCoE network as a virtual expansion port (VE_Port).
  - Tag the VE_Port to the FCoE VLAN that will carry traffic through the tunnel.
  - Configure the FC port that will connect to an E_Port on an FC as a TE_Port.
  - Use this command (**fcoe e-tunnel**) with the **fc-port1** and **vlan** parameters to associate the TE_Port with the FCoE VLAN to which the VE_Port is tagged.
- To create a tunnel between two FC TE_Ports on the same switch or in a virtual chassis configuration, use the **fc-port1** and **fc-port2** parameters to specify the slot and port number of the two TE ports.

Examples

```
-> fcoe e-tunnel 1 fc-port1 2/1 fc-port2 2/2
-> fcoe e-tunnel 10 fc-port1 2/3 vlan 200
-> fcoe e-tunnel 11 fc-port1 2/4 vlan 200
-> no fcoe e-tunnel 10
```

Release History

Release 7.3.3; command introduced.

Related Commands

fcoe vlan	Configures an FCoE VLAN.
fcoe role	Configures an FCoE port as a VE_Port.
fibre-channel port mode	Configures an FC port as a TE_Port
show fcoe e-tunnel	Displays the E2E tunnel configuration.
show fibre-channel sessions	Displays FC sessions on FC ports.

MIB Objects

```
alaFipsEtunnelTable
   alaFipsEtunnelVlanId
   alaFipsEtunnelIfIndexOne
   alaFipsEtunnelIfIndexTwo
   alaFipsEtunnelRowStatus
```

show fibre-channel vsan

Displays the VSAN configuration for the switch.

show fibre-channel vsan [*vsan_id***]-***vsan_id2***]**

Syntax Definitions

*vsan_id***[-***vsan_id2***]**	An existing VSAN ID. Use a hyphen to specify a range of VSAN IDs (10-25).

Defaults

By default, a list of all VSANs is displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Specify a VSAN ID with this command to display information about a specific VSAN.

Examples

```
-> show fibre-channel vsan

 vsan  oper admin  name
------+----+-----+---------
    1  Ena   Dis  test1
 1000  Dis   Dis  test2
 2000  Ena   Dis  test3

-> show fibre-channel vsan 101

vsan  oper admin  name
------+----+-----+---------
 1000  Dis   Dis  test2
```

output definitions

vsan	The numerical VSAN ID.
oper	The operational status of the VSAN: **Ena** (enabled) or **Dis** (disabled). The operational status remains disabled until an active FC port is assigned to the VSAN. A VSAN must have an enabled administrative status before it can become operationally enabled.
admin	The administrative status of the VSAN: **Ena** specifies that VSAN functions are enabled; **Dis** specifies that VLAN functions are disabled.
name	The user-defined text description for the VSAN. By default, the VSAN ID is displayed if the VLAN description is not specified.

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel vsan	Configures a VSAN for the switch.
show fibre-channel vsan members	Displays VSAN port assignments.

MIB Objects

```
alaFcVsanTable
   alaFcVsanNumber
   alaFcVsanDescription
   alaFcVsanAdmStatus
   alaFcVsanOperStatus
   alaFcVsanRowStatus
```

show fibre-channel vsan members

Displays the VSAN port assignments.

show fibre-channel vsan [*vsan_id* **[-***vsan_id2***]] members [port** *chassis/slot/port***[-***port2***]]**

Syntax Definitions

vsan_id[-*vsan_id2*]	An existing VSAN ID number. Use a hyphen to specify a range of VSAN IDs (10-25).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

Defaults

By default, all VSAN port assignments are displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- If the *vsan_id* is specified without a *slot/port*, then all port assignments for that VSAN are displayed.
- If both the *vsan_id* and *slot/port* are specified, then information only for that VSAN and slot/port is displayed.
- Only OmniSwitch FC ports can be assigned to a VSAN.

Examples

```
-> show fibre-channel vsan members
 vsan   port  status
------+------+--------
    1  2/2/1   Enabled
 1003  2/2/12  Enabled
 1005  3/2/5   Disbled

-> show fibre-channel vsan 1003 members
  port   status
-------+--------
 2/2/12  Enabled

-> show fibre-channel vsan 1005 members port 3/2/5
vsan   : 1005,
port   : 3/2/5,
status : disabled
```

output definitions

vsan	The numerical VSAN ID. Configured through the **fibre-channel vsan** command.
port	The FC port number associated with the VSAN ID. Configured through the **fibre-channel vsan members** command.
status	The operational status of the port (**enabled** or **disabled**).

Release History

Release 7.3.3; command introduced.

Related Commands

show fibre-channel vsan	Displays the VSAN configuration for the switch.

MIB Objects

```
alaFcVfpaTable
   alaFcVfpaVsanNumber
   alaFcVfpaIfIndex
   alaFcVfpaState
   alaFcVfpaRowStatus
```

show fibre-channel port

Displays the FC port configuration for the switch.

show fibre-channel port [info]

Syntax Definitions

info	Displays session details for each FC port.

Defaults

By default, the parameters for each FC port are displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When the **info** parameter is used with this command, the **fcid** field shows an FC port ID for NP_Ports. For all other port modes, this field is blank. Only NP_Ports perform fabric login (FLOGI) and obtain a port ID from an FC switch.
- If an FC port is configured to operate in the fabric or tunnel E_Port mode, there is no fabric login process performed. Ports running in these modes will come up immediately.
- FLOGI is triggered only after an NP_Port is assigned to a VSAN.

Examples

```
-> show fibre-channel port
Legend: NP=Proxy N_Port, F=Fabric Port connected to N_port, TE=Tunnel E-Port

ports   oper-status mode  BB-SC-N  service class
-------+-----------+-----+-------+---------------
  2/1        Up      NP        3              3
  2/2        Up      F         0              3
  2/3        Up      TE        3            3/F
  2/4       Down     NP        0              3
```

output definitions

ports	The slot and port number of the FC port.
oper-status	The operational status of the FC port.
mode	The operational mode for the FC port.
BB-SC-N	The buffer-to-buffer state change number configured for the FC port.
service class	The service class for the FC port session (**2**, **3**, **F**, or **3/F**). This value indicates the level of delivery integrity required for an application.

```
-> show fibre-channel port info
Legend: NP=Proxy N_Port, F=Fabric Port connected to N_port, TE=Tunnel E-Port

 ports  mode  fcid        wwpn                state
-------+----+-------+----------------------+----------
   2/1   NP  010010c 10:00:01:00:00:0a:22:11 Up
   2/2   F       -   10:00:01:00:00:0b:22:1a Up
   2/3   TE      -   10:00:01:00:00:0b:23:22 Up
   2/4   NP      -   10:00:01:00:00:0b:23:23 FLOGI_Sent
   2/5   NP      -   10:00:01:00:00:0b:23:24 Not_Init
```

output definitions

ports	The slot and port number of the FC port.
mode	The operational mode for the FC port (**NP** = proxy N_Port, **F** = fabric port, **TE** = tunnel E_Port). Configured through the **fibre-channel port mode** command.
fcid	The FC port_ID obtained after successful fabric login. This field applies only to NP_Ports.
wwpn	The world-wide port name assigned to the OmniSwitch FC port.
state	The operational state of the fabric login process (**Up**, **Down**, **FLOGI_Sent**, **Not_Init**, **ELP_Sent**, **Sess_Clear**).

Release History

Release 7.3.3; command introduced.

Related Commands

show fibre-channel vsan	Displays the VSAN configuration for the switch.
show fibre-channel vsan members	Displays the VSAN port assignments for the switch.

MIB Objects

```
alaFcIntfTable
   alaFcIntfIfIndex
   alaFcIntfOperStatus
   alaFcIntfMode
   alaFcIntfBbScN
   alaFcIntfBbCredit
   alaFcIntfBbRxDataField
   alaFcIntfClassOfService
   alaFcIntfFcid
   alaFcIntfWwpn
   alaFcIntfLoginState
   alaFcIntfRowStatus
```

show fcoe vsan-map

Displays the VSAN-to-FCoE VLAN mapping configuration.

show fcoe vsan-map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Mapping a VSAN to an FCoE VLAN is required to activate the processing of specific ENode traffic traveling to and from the designated virtual FC fabric through the NPIV OmniSwitch.

Examples

```
-> show fcoe vsan-map
 vsan   vlan
------+-----
    10    10
  2000  2000
  3000  3000
```

output definitions

vsan	The VSAN ID. Configured through the **fibre-channel vsan** command**.**
vlan	The FCoE VLAN ID. Configured through the **fcoe vlan** command**.**

Release History

Release 7.3.3; command introduced.

Related Commands

fcoe vsan-map	Configures a one-to-one mapping between a VSAN and FCoE VLAN.
show vlan	Displays the FCoE VLAN configuration.

MIB Objects

```
alaFipsVsanVlanMapTable
   alaFipsVsanVlanMapVsanNumber
   alaFipsVsanVlanMapVlanNumber
   alaFipsVsanVlanMapRowStatus
```

show fibre-channel sessions

Displays the sessions established on the OmniSwitch FC ports.

show fibre-channel sessions [vsan *vsan_id* **| e-tunnel** *tunnel_id***] [port** *chassis/slot/port***] [summary]**

Syntax Definitions

vsan_id	An existing VSAN ID number.
tunnel_id	An existing E-Tunnel (E2E Tunnel) ID.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1).

Defaults

By default, all FC sessions are displayed for all FC ports.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

The **port** parameter can be combined with the **vsan** or **e-tunnel** parameters to display sessions for a specific FC port within a VSAN or E2E tunnel.

Examples

```
-> show fibre-channel sessions summary
Total FIBRE-CHANNEL Sessions               : 7    ,
Total NPIV Sessions                        : 4    ,
Total R-NPIV Sessions                      : 1    ,
Total E-TUNNEL Sessions                    : 2

-> show fibre-channel sessions
Total FIBRE-CHANNEL Sessions               : 4
Total NPIV Sessions                        : 2
Total R-NPIV Sessions                      : 1
Total E-TUNNEL Sessions                    : 1

 Port    Mode VSAN T-ID       WWPN               FCID   Status   Login Type
--------+----+----+----+----------------------+--------+--------+-------------
 2/1     NP   100   -   11:00:00:17:A4:B1:71:23 00:01:01  SUCCESS    FLOGI
 2/2     F    200   -   11:00:00:17:A4:B1:72:24 00:01:02  SUCCESS    FLOGI
 2/1     NP   100   -   11:00:00:17:A4:B1:71:24 00:01:03  SUCCESS    FDISC
 2/3     TE    -    -   11:00:00:17:A4:B1:71:2a     -     SUCCESS    ELP

-> show fibre-channel sessions vsan 200
 Port    Mode VSAN T-ID       WWPN               FCID   Status   Login Type
--------+----+----+----+----------------------+--------+--------+-------------
 2/2     F    200   -   11:00:00:17:A4:B1:72:24 00:01:02  SUCCESS    FLOGI
```

```
-> show fibre-channel sessions port 2/1
 Port    Mode VSAN T-ID       WWPN                FCID   Status   Login Type
--------+----+----+----+----------------------+--------+--------+-------------
 2/1     NP   100   -   11:00:00:17:A4:B1:71:23 00:01:01  SUCCESS    FLOGI
 2/1     NP   100   -   11:00:00:17:A4:B1:71:24 00:01:03  SUCCESS    FDISC

-> show fibre-channel sessions e-tunnel 10
 Port    Mode VSAN T-ID       WWPN                FCID   Status   Login Type
--------+----+----+----+----------------------+--------+--------+-------------
  2/3    TE    -    10  11:00:00:17:A4:B1:71:2a     -     SUCCESS    ELP
  2/4    TE    -    10  11:00:00:17:A4:B1:71:2b     -     SUCCESS    ELP

-> show fibre-channel sessions e-tunnel 10 port 2/3
 Port    Mode VSAN T-ID       WWPN                FCID   Status   Login Type
--------+----+----+----+----------------------+--------+--------+-------------
  2/3    TE    -    10  11:00:00:17:A4:B1:71:2a     -     SUCCESS    ELP

-> show fibre-channel sessions port 2/3
 Port    Mode VSAN T-ID       WWPN                FCID   Status   Login Type
--------+----+----+----+----------------------+--------+--------+-------------
  2/3    TE    -    10  11:00:00:17:A4:B1:71:2a     -     SUCCESS    ELP
```

output definitions

Port	The slot and port number for the FC port.
Mode	The operational mode for the FC port (**F** = F_Port, **NP** = proxy N_Port, **TE** = tunnel E_Port). Configured through the **fibre-channel port mode**.
vsan	The VSAN ID to which the NP_Port or F_Port is assigned. Configured through the **fibre-channel vsan** command**.**
T-ID	The E2E tunnel ID. Configured through the **fcoe e-tunnel** command.
WWPN	The world-wide port name associated with the OmniSwitch FC port.
FCID	The FC port ID assigned to the node during login.
Status	The status of the login session.
Login Type	The type of login (FLOGI = fabric login, FDISC = fabric discovery, or ELP = exchange link parameters).

Release History

Release 7.3.3; command introduced.

Related Commands

clear fibre-channel sessions	Clears FC sessions.
show fibre-channel node	Displays a list of FC nodes connected through the switch.

MIB Objects

```
alaFcSessTable
   alaFcSessIfIndex
   alaFcSessVsanNumber,
   alaFcSessStatus,
   alaFcSessIntfMode,
   alaFcSessFcid,
   alaFcSessWwpn,
   alaFcSessType,
   alaFcSessTunnelId
```

show fibre-channel node

Displays a list of FC nodes connected to OmniSwitch FC ports.

show fibre-channel node [vsan *vsan_id* **| port** *chassis/slot/port***]**

Syntax Definitions

vsan_id	An existing VSAN ID number.
chassis	The chassis identifier.
slot/port	The slot and port number (3/1).

Defaults

By default, a list of all FC nodes is displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Specify a VSAN ID to display nodes associated with a specific VSAN.
- Specify an FC port number to display nodes connected on a specific FC port.

Examples

```
-> show fibre-channel node
VSAN  VLAN       WWNN                     WWPN               Port   FC-ID
-----+-----+----------------------+----------------------+------+--------
1     200   20:00:00:24:FF:37:DD:BB 21:00:00:24:FF:37:DD:BB  2/7   02:09:02
10    100   11:00:00:17:A4:B1:71:23 11:00:00:17:A4:B1:71:23  2/1   00:0A:01
10     -    11:00:00:17:A4:B1:71:24 11:00:00:17:A4:B1:71:24  2/2   00:0B:02

-> show fibre-channel node vsan 10

VSAN  VLAN       WWNN                WWPN                   Port    FC-ID
-----+-----+-----------------------+----------------------+------+-------
10    100   11:00:00:17:A4:B1:71:23  11:00:00:17:A4:B1:71:23  2/1   00:0A:01
10     -    11:00:00:17:A4:B1:71:24  11:00:00:17:A4:B1:71:24  2/2   00:0B:02

-> show fibre-channel node port 2/1

 Port   VSAN  VLAN       WWNN                WWPN                   FC-ID
------+-----+-----+----------------------+----------------------+-------
 2/1      10   100 11:00:00:17:A4:B1:71:23 11:00:00:17:A4:B1:71:23  00:0A:01
```

output definitions

Port	The slot/port of the FC interface that is connected to the FC node.
VSAN	The VSAN ID associated with the FC node. Configured through the **fibre-channel vsan** command.
VLAN	The FCoE VLAN ID on which FC nodes are provided. Configured through the **fcoe vlan** command.
WWNN	The world-wide node name assigned to an FC node.
WWPN	The world-wide port name assigned to the FC port.
FC-ID	The FC port ID assigned to an N_Port (or VN_Port, or NP_Port) after successful fabric login.

Release History

Release 7.3.3; command introduced.

Related Commands

show fibre-channel sessions	Displays the sessions established on the OmniSwitch FC ports.

MIB Objects

```
alaFcNodeTable
   alaFcNodeIfIndex
   alaFcNodeVsanNumber
   alaFcNodeVlanNumber
   alaFcNodeFci
   alaFcNodeWwpn
   alaFcNodeWwnn
```

show fcoe e-tunnel

Displays the E2E tunnel configuration for the switch.

show fcoe e-tunnel [*tunnel_id***]**

Syntax Definitions

tunnel_id	An existing tunnel ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the *tunnel_id* to display parameters for a specific tunnel.

Examples

```
-> show fcoe e-tunnel

 tunnel  vlan  Port1   Port2
-------+-----+-------+----------
     1   1000  1/1/1     -
     2     -   1/1/2   3/3/1
     3   3000  1/1/3     -

-> show fcoe e-tunnel 2
 tunnel  vlan  Port1   Port2
-------+-----+-------+----------
     2     -   1/1/2   3/3/1
```

output definitions

Tunnel	The E2E tunnel ID associated with the session. Configured through
Vlan	The FCoE VLAN on which the tunnel is defined. Configured through the **fcoe vlan** command.
Port1, Port2	The FCoE port (in VE_Port role) and/or FC port (in TE_Port mode) for this session. The FCoE port rule is configured through the **fcoe role** command. The FC port mode is configured through the **fibre-channel port mode** command.

Release History

Release 7.3.3; command introduced.

Related Commands

fcoe e-tunnel	Configures E2E tunnel parameters.

MIB Objects

```
alaFipsEtunnelTable
   alaFipsEtunnelId
   alaFipsEtunnelVlanId
   alaFipsEtunnelIfIndexOne
   alaFipsEtunnelIfIndexTwo
```

show fibre-channel

Displays global Fibre Channel parameter values.

show fibre-channel

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

This command currently displays the following:

- The load-balancing method that is applied to FLOGI requests when there is more than one NPIV proxy port assigned to the same VSAN. This mode does not apply to FC ports configured to operate in the F_Port proxy mode (R-NPIV) or as E2E tunnel ports.
- The World Wide Node Name (WWNN) for the switch. The WWNN is comprised of “10:00” combined with the next available increment of the switch based MAC address.

Examples

```
-> show fibre-channel
Fibre Channel Global Configurations     :
----------------------------------------
NPIV Proxy Global Load Balance Method   : Default
Local WWNN                              : 10:00:00:E0:B1:E7:09:A4
```

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel npiv-proxy load-balance	Configures the load balancing method applied to multiple FC ports that belong to the same VSAN.

MIB Objects

```
alaFipsEtunnelTable
   alaFipsEtunnelId
   alaFipsEtunnelVlanId
   alaFipsEtunnelIfIndexOne
   alaFipsEtunnelIfIndexTwo
```

show fibre-channel statistics

Displays FC port statistics.

show fibre-channel statistics [npiv | r-npiv] [vsan *vsan_id***[***vsan_id2***] [port** *chassis/slot/port***[-***port2***] [e-tunnel port** *chassis/slot/port***[-***port2***]]**

Syntax Definitions

npiv	Displays statistics for N_Port proxy sessions**.**
r-npiv	Displays statistics for F_Port proxy sessions.
e-tunnel [*tunnel_id***]**	Displays E2E tunnel (E_Port proxy) statistics. Optionally enter a tunnel ID to display information for a specific tunnel.
*vsan_id***[***vsan_id2***]**	An existing VSAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VSAN IDs (100-150).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

Defaults

By default, all statistics are displayed

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **vsan** parameter to display statistics for a specific VSAN ID. The **vsan** parameter is not used with the **e-tunnel** parameter, because tunnel ports are not associated with a VSAN.
- Use the **port** parameter to display statistics for a specific FC port.

Examples

```
-> show fibre-channel statistics vsan 46
NPIV VSAN Statistics:

Packets Received:
 VSAN    LS_ACC    FLOGO      LS_RJT
------+----------+----------+----------
    46        29         0         0

Packets Sent:
 VSAN     FLOGI       FDISC     FLOGO
------+----------+----------+----------
    46         5        18        14

R-NPIV VSAN Statistics:
Packets Received:
```

```
 VSAN      FLOGI      FDISC     FLOGO
--------+----------+----------+----------
      46         0         0         0

Packets Sent:
 VSAN     FLOGI_ACC FLOGI_RJT  FDISC_ACC  FDISC_RJT   FLOGO
--------+----------+----------+----------+----------+----------
      46         0         0         0         0         0

-> show fibre-channel statistics npiv vsan 46
NPIV VSAN Statistics:

Packets Received:
 VSAN    LS_ACC    FLOGO      LS_RJT
------+----------+----------+----------
    46        29         0         0

Packets Sent:
 VSAN     FLOGI       FDISC     FLOGO
------+----------+----------+----------
    46         5        18        14

-> show fibre-channel statistics e-tunnel port 1/2/3

E-Tunnel Port Statistics
Packets Received:
 Port       Tunnel     ELP        SW_ACC      SW_RJT
----------+----------+----------+----------+----------
     1/2/3         2         3         0         2

Packets Sent:
 Port       Tunnel     ELP        SW_ACC     SW_RJT
----------+----------+----------+----------+----------
     1/2/3         2      9483         3         0
```

Release History

Release 7.3.3; command introduced.

Related Commands

clear fibre-channel statistics Clears FC port statistics.

MIB Objects

```
 alaFcIntfNpivStatsTable
   alaFcIntfNpivStatsIfIndex
   alaFcIntfNpivStatsFlogis
   alaFcIntfNpivStatsFdiscs
   alaFcIntfNpivStatsFlogiAccs
   alaFcIntfNpivStatsFdiscAccs
   alaFcIntfNpivStatsFlogos
   alaFcIntfNpivStatsFlogiRjts
   alaFcIntfNpivStatsFdiscRjts
alaFcVsanNpivStatsTable
   alaFcVsanNpivStatsVsan
   alaFcVsanNpivStatsFlogis
   alaFcVsanNpivStatsFdiscs
   alaFcVsanNpivStatsFlogiAccs
   alaFcVsanNpivStatsFdiscAccs
   alaFcVsanNpivStatsFlogos
   alaFcVsanNpivStatsFlogiRjts
   alaFcVsanNpivStatsFdiscRjts
alaFcIntfRnpivStatsTable
   alaFcIntfRnpivStatsIfIndex
   alaFcIntfRnpivStatsFlogis
   alaFcIntfRnpivStatsFdiscs
   alaFcIntfRnpivStatsFlogiLsAccs
   alaFcIntfRnpivStatsFdiscLsAccs
   alaFcIntfRnpivStatsFlogos
   alaFcIntfRnpivStatsFlogiRjts
   alaFcIntfRnpivStatsFdiscRjts
alaFcVsanRnpivStatsTable
   alaFcVsanRnpivStatsVsan
   alaFcVsanRnpivStatsFlogis
   alaFcVsanRnpivStatsFdiscs
   alaFcVsanRnpivStatsFlogiLsAccs
   alaFcVsanRnpivStatsFdiscLsAccs
   alaFcVsanRnpivStatsFlogos
   alaFcVsanRnpivStatsFlogiRjts
   alaFcVsanRnpivStatsFdiscRjts
alaFcTidEtunnelStatsTable
   alaFcTidEtunnelStatsTunnelId
   alaFcTidEtunnelStatsElpReqs
   alaFcTidEtunnelStatsSwAccs
   alaFcTidEtunnelStatsSwRjts
alaFcIntfEtunnelStatsTable
   alaFcIntfEtunnelStatsIfIndex
   alaFcIntfEtunnelStatsElpReqs
   alaFcIntfEtunnelStatsSwAccs
   alaFcIntfEtunnelStatsSwRjts
```

show fcoe statistics npiv-proxy

Displays ENode fabric login or ENode discovery statistics for FCoE interfaces or specific VLANs.

show fcoe statistics npiv-proxy {enode-login | enode-discovery} {interface | vlan [*vlan_id***[***vlan_id2***] | port** *chassis/slot/port***[-***port2***]** | **linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

enode-login	Displays ENode login statistics**.**
enode-discovery	Displays ENode discovery statistics.
interface	Display statistics for all FCoE interfaces (ports and link aggregates).
*vlan_id***[***vlan_id2***]**	An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VLAN IDs (100-150).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **vlan** parameter to display statistics for a specific FCoE VLAN ID.
- Use the **port** or **linkagg** parameters to display statistics for a specific FCoE port or link aggregate ID.

Examples

```
->show fcoe statistics npiv-proxy enode-discovery interface
Packets Received:
 Port    Vlan Req     MDS       UDS
-------+----------+----------+---------
  1/1            1      1         0
  1/22           1      1         0
Packets Sent:
 Port    Vlan Res      MDA       UDA
-------+----------+----------+---------
  1/1            1      3         1
  1/22           1      3         1
```

```
-> show fcoe statistics npiv-proxy enode-login interface
Packets Received:
   Port     FLOGI     FDISC      LOGO     E_KA      VN_KA
---------+---------+---------+---------+---------+---------
 1/12             0         0         0         0         0
Packets Sent:
   Port   FLOGI_ACC FDISC_ACC FLOGO_ACC FLOGI_RJT FDISC_RJT FLOGO_RJT    CVL
---------+---------+---------+---------+---------+---------+---------+---------
 1/12             0         0         0         0         0         0         0
```

Release History

Release 7.3.3; command introduced.

Related Commands

clear fcoe statistics npiv	Clears ENode and FCF statistics.

MIB Objects

```
alaFipsVlanNpivDiscStatsTable
   alaFipsVlanNpivDiscStatsVlanId
   alaFipsVlanNpivDiscStatsVlanDiscRqs
   alaFipsVlanNpivDiscStatsVlanDiscResps
   alaFipsVlanNpivDiscStatsMdss
   alaFipsVlanNpivDiscStatsUdss
   alaFipsVlanNpivDiscStatsMdas
   alaFipsVlanNpivDiscStatsUdas
   alaFipsVlanNpivDiscStatsVnkas
alaFipsIntfNpivDiscStatsTable
   alaFipsIntfNpivDiscStatsIfIndex
   alaFipsIntfNpivDiscStatsVlanDiscRqs,
   alaFipsIntfNpivDiscStatsVlanDiscResps
   alaFipsIntfNpivDiscStatsMdss
   alaFipsIntfNpivDiscStatsUdss
   alaFipsIntfNpivDiscStatsMdas
   alaFipsIntfNpivDiscStatsUdas
   alaFipsIntfNpivDiscStatsVnkas
alaFipsVlanNpivLoginStatsTable
   alaFipsVlanNpivLoginStatsVlanId
   alaFipsVlanNpivLoginStatsFlogis
   alaFipsVlanNpivLoginStatsFdiscs
   alaFipsVlanNpivLoginStatsLsAccs
   alaFipsVlanNpivLoginStatsLsRjts
   alaFipsVlanNpivLoginStatsLogos
   alaFipsVlanNpivLoginStatsCvls
   alaFipsVlanNpivLoginStatsEkas
   alaFipsVlanNpivLoginStatsVnkas
alaFipsIntfNpivLoginStatsTable
   alaFipsIntfNpivLoginStatsIfIndex
   alaFipsIntfNpivLoginStatsFlogis
   alaFipsIntfNpivLoginStatsFdiscs
   alaFipsIntfNpivLoginStatsLsAccs
   alaFipsIntfNpivLoginStatsLsRjts
   alaFipsIntfNpivLoginStatsLogos
   alaFipsIntfNpivLoginStatsCvls
   alaFipsIntfNpivLoginStatsEkas
   alaFipsIntfNpivLoginStatsVnkas
```

show fcoe statistics r-npiv

Displays FCF discovery fabric login or ENode discovery statistics for FCoE interfaces or specific VLANs.

show fcoe statistics r-npiv {node-login | fcf-discovery} {interface | vlan [*vlan_id***[***vlan_id2***] | port** *chassis/slot/port***[-***port2***]** | **linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

node-login	Displays FC node login statistics**.**
fcf-discovery	Displays FCF discovery statistics.
interface	Display statistics for all FCoE interfaces (ports and link aggregates).
*vlan_id***[***vlan_id2***]**	An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VLAN IDs (100-150).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **vlan** parameter to display statistics for a specific FCoE VLAN ID.
- Use the **port** or **linkagg** parameters to display statistics for a specific FCoE port or link aggregate ID.

Examples

```
-> show fcoe statistics r-npiv fcf-discovery interface
Packets Received:
 Port      MDA       UDA
---------+---------+---------
 1/1              1         4
 1/5              8         3
Packets Sent :
  Port      MDS       UDS
---------+---------+---------
 1/1           1          4
 1/5           8          3
```

```
-> show fcoe statistics r-npiv fcf-discovery linkagg 2
Packets Received:
   Port      MDA       UDA
---------+---------+---------
 0/2           3167         1
Packets Sent:
   Port      MDS       UDS
---------+---------+---------
 0/2              0         1

-> show fcoe statistics r-npiv node-login interface
Packets Received:
   Port   FLOGI_ACC FDISC_ACC FLOGI_RJT FDISC_RJT   CVL
---------+---------+---------+---------+---------+---------
  1/2            1         4         3         1         0
  1/5            8         3         3         1         0
Packets Sent:
   Port     FLOGI     FDISC     LOGO      VN-KA     E-KA
---------+---------+---------+---------+---------+---------
  1/2            1         6         1         7         1
  1/5            2         1         8         3         3

-> show fcoe statistics r-npiv node-login linkagg 2
Packets Received:
   Port   FLOGI_ACC FDISC_ACC FLOGI_RJT FDISC_RJT   CVL
---------+---------+---------+---------+---------+---------
 0/2              3         0         0         0         0
Packets Sent:
   Port     FLOGI     FDISC     LOGO      VN-KA     E-KA
---------+---------+---------+---------+---------+---------
 0/2              1         0         0       271      3048
```

Release History

Release 7.3.3; command introduced.

Related Commands

clear fcoe statistics r-npiv	Clears ENode and FCF statistics.

MIB Objects

```
alaFipsVlanRnpivDiscStatsTable
   alaFipsVlanRnpivDiscStatsVlanId
   alaFipsVlanRnpivDiscStatsMdss
   alaFipsVlanRnpivDiscStatsUdss
   alaFipsVlanRnpivDiscStatsMdas
   alaFipsVlanRnpivDiscStatsUdas
   alaFipsIntfRnpivDiscStatsTable
   alaFipsIntfRnpivDiscStatsIfIndex
   alaFipsIntfRnpivDiscStatsMdss
   alaFipsIntfRnpivDiscStatsUdss
   alaFipsIntfRnpivDiscStatsMdas
   alaFipsIntfRnpivDiscStatsUdas
alaFipsVlanRnpivLoginStatsTable
   alaFipsVlanRnpivLoginStatsVlanId
   alaFipsVlanRnpivLoginStatsFlogis
   alaFipsVlanRnpivLoginStatsFdiscs
   alaFipsVlanRnpivLoginStatsLsAccs
   alaFipsVlanRnpivLoginStatsFlogiLsRjts
   alaFipsVlanRnpivLoginStatsFdiscLsRjts
   alaFipsVlanRnpivLoginStatsCvls
   alaFipsVlanRnpivLoginStatsLogos
   alaFipsVlanRnpivLoginStatsVnkas
   alaFipsVlanRnpivLoginStatsEkas
   alaFipsVlanRnpivLoginStatsClear
alaFipsIntfRnpivLoginStatsTable
   alaFipsIntfRnpivLoginStatsIfIndex
   alaFipsIntfRnpivLoginStatsFlogis
   alaFipsIntfRnpivLoginStatsFdiscs
   alaFipsIntfRnpivLoginStatsLsAccs
   alaFipsIntfRnpivLoginStatsFlogiLsRjts
   alaFipsIntfRnpivLoginStatsFdiscLsRjts
   alaFipsIntfRnpivLoginStatsCvls
   alaFipsIntfRnpivLoginStatsLogos
   alaFipsIntfRnpivLoginStatsVnkas
   alaFipsIntfRnpivLoginStatsEkas
```

show fcoe statistics e-tunnel

Displays E2E tunnel statistics.

show fcoe statistics e-tunnel [ve | te] [*tunnel_id***[-***tunnel_id***]]**

Syntax Definitions

ve	Displays VE_Port statistics**.**
te	Displays TE_Port statistics.
*tunnel_id***[-***tunnel_id***]**	The ID of an existing E2E tunnel. Use a hyphen to specify a range of tunnel IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **vlan** parameter to display statistics for a specific FCoE VLAN ID.
- Use the **port** or **linkagg** parameters to display statistics for a specific FCoE port or link aggregate ID.

Examples

```
-> show fcoe statistics e-tunnel

Packet Received :
Tunnel   ELP    SW_ACC   SW_RJT
------+--------+--------+--------
 15     7        1        6
 17     5        4        1
Packet Sent :
Tunnel   ELP    SW_ACC   SW_RJT
------+--------+--------+--------
 15     7        1        6
 17     5        4        1

Packet Recevied :
Tunnel   MDS    UDS     MDA     UDA   ELP_REQ SW_ACC  SW_RJT  CVL
------+------+-------+-------+-------+-------+-------+-------+-------
 15        1       6       1       4       3       1       1       7
 17        2       1       8       3       3       1       5       9
Packet Sent :
Tunnel   MDS    UDS     MDA     UDA   ELP_REQ SW_ACC  SW_RJT  CVL
------+------+-------+-------+-------+-------+-------+-------+-------
 15        1       6       1       4       3       1       1       7
 17        2       1       8       3       3       1       5       9
```

```
-> show fcoe statistics e-tunnel te

Packet Received :
Tunnel   ELP    SW_ACC   SW_RJT
------+--------+--------+--------
 15     7        1        6
 17     5        4        1
Packet Sent :
Tunnel   ELP    SW_ACC   SW_RJT
------+--------+--------+--------
 15     7        1        6
 17     5        4        1

-> show fcoe statistics e-tunnel te 17

Packet Received :
Tunnel   ELP    SW_ACC   SW_RJT
------+--------+--------+--------
 17     5        4        1
Packet Sent :
Tunnel   ELP    SW_ACC   SW_RJT
------+--------+--------+--------
 17     5        4        1

-> show fcoe statistics e-tunnel ve

Packet Recevied :
Tunnel   MDS    UDS     MDA     UDA   ELP_REQ SW_ACC  SW_RJT  CVL
------+------+-------+-------+-------+-------+-------+-------+-------
 15        1       6       1       4       3       1       1       7
 17        2       1       8       3       3       1       5       9
Packet Sent :
Tunnel   MDS    UDS     MDA     UDA   ELP_REQ SW_ACC  SW_RJT  CVL
------+------+-------+-------+-------+-------+-------+-------+-------
 15        1       6       1       4       3       1       1       7
 17        2       1       8       3       3       1       5       9

-> show fcoe statistics e-tunnel ve 17

Packet Recevied :
Tunnel   MDS    UDS     MDA     UDA   ELP_REQ SW_ACC  SW_RJT  CVL
------+------+-------+-------+-------+-------+-------+-------+-------
 17        2       1       8       3       3       1       5       9
Packet Sent :
Tunnel   MDS    UDS     MDA     UDA   ELP_REQ SW_ACC  SW_RJT  CVL
------+------+-------+-------+-------+-------+-------+-------+-------
 17        2       1       8       3       3       1       5       9
```

Release History

Release 7.3.3; command introduced.

Related Commands

clear fcoe statistics e-tunnel	Clears ENode and FCF statistics.

MIB Objects

```
alaFipsEtunnelVePortStatsTable
   alaFipsEtunnelVePortStatsTunnelId
   alaFipsEtunnelVePortStatsIfIndex
   alaFipsEtunnelVePortStatsMdss
   alaFipsEtunnelVePortStatsUdss
   alaFipsEtunnelVePortStatsMdas
   alaFipsEtunnelVePortStatsUdas
   alaFipsEtunnelVePortStatsElpReqs
   alaFipsEtunnelVePortStatsSwAccs
   alaFipsEtunnelVePortStatsSwRjts
   alaFipsEtunnelVePortStatsCvls
alaFipsEtunnelTePortStatsTable
   alaFipsEtunnelTePortStatsTunnelId
   alaFipsEtunnelTePortStatsIfIndex
   alaFipsEtunnelTePortStatsElpReqs
   alaFipsEtunnelTePortStatsSwAccs
   alaFipsEtunnelTePortStatsSwRjts
```

show fibre-channel npiv-proxy load-balance

Displays the NPIV proxy load balancing static mapping and session count.

show fibre-channel npiv-proxy load balance {static | session-count}

Syntax Definitions

static	Displays the static FCoE port/FC NP_Port mapping.
session-count	Displays the number of sessions on each FC port.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- This command displays information only for FC ports operating in the NP_Port mode.
- Use the **static** parameter to display only the static mapping of FCoE ports to FC NP_Ports.
- When the **sessions-count** parameter is used, the “FC Port” field includes all NP_Ports.

Examples

```
-> show fibre-channel npiv-proxy load-balance static

FCoE Port   FC port
-----------+---------
 1/1        2/1
 1/2        2/1

-> show fibre-channel npiv-proxy load-balance sessions-count

 FC Port  session_count
--------+--------------
  2/1                2
  2/2                0
  2/3                5
```

output definitions

FCoE Port	The slot/port of the FCoE port that is mapped to the FC port.
FC Port	The slot/port of the FC NP_Port.
Session Count	The number of sessions per FC port.

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel npiv-proxy load-balance static	Configures a static mapping between an FCoE port and an FC NP_Port.
fibre-channel npiv-proxy load-balance	Configures the NPIV proxy load-balancing method applied to all FC NP_Ports on the switch.

MIB Objects

```
alaFcNpivStaticLoadBalanceTable
   alaFcNpivStaticLoadBalanceFibreIfIndex
   alaFcNpivStaticLoadBalanceEtherIfIndex
   alaFcNpivStaticLoadBalanceRowStatus
alaFcNpivLoadBalSessTable
   alaFcNpivLoadBalSessIfIndex
   alaFcNpivLoadBalSessCount
```

clear fibre-channel statistics

Clears FC port statistics.

clear fibre-channel statistics [npiv | r-npiv] [port *chassis/slot/port***[**-*port2***] [e-tunnel port** *chassis/slot/port***[**-*port2***]]**

Syntax Definitions

npiv	Clears statistics for N_Port proxy sessions**.**
r-npiv	Clears statistics for F_Port proxy sessions.
e-tunnel [*tunnel_id***]**	Clears E2E tunnel (E_Port proxy) statistics. Optionally enter a tunnel ID to display information for a specific tunnel.
*vsan_id***[***vsan_id2***]**	An existing VSAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VSAN IDs (100-150).
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

Defaults

By default, all statistics are cleared.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **vsan** parameter to clear statistics for a specific VSAN ID. The **vsan** parameter is not used with the **e-tunnel** parameter, because tunnel ports are not associated with a VSAN.
- Use the **port** parameter to clear statistics for a specific FC port.

Examples

```
-> clear fibre-channel statistics
-> clear fibre-channel statistics port 2/2/5
-> clear fibre-channel statistics npiv
-> clear fibre-channel statistics r-npiv
-> clear fibre-channel statistics e-tunnel
-> clear fibre-channel statistics npiv port 2/2/1
-> clear fibre-channel statistics r-npiv port 2/2/3
-> clear fibre-channel statistics e-tunnel port 2/2/4
```

Release History

Release 7.3.3; command introduced.

Related Commands

show fibre-channel statistics	Display FC port statistics.

MIB Objects

```
alaFcIntfNpivStatsTable
   alaFcIntfNpivStatsIfIndex
   alaFcIntfNpivStatsClear
alaFcVsanNpivStatsTable
   alaFcVsanNpivStatsVsan
   alaFcVsanNpivStatsClear
alaFcIntfRnpivStatsTable
   alaFcIntfRnpivStatsIfIndex
   alaFcIntfRnpivStatsClear
alaFcVsanRnpivStatsTable
   alaFcVsanRnpivStatsVsan
   alaFcVsanRnpivStatsClear
alaFcTidEtunnelStatsTable
   alaFcTidEtunnelStatsTunnelId
   alaFcTidEtunnelStatsClear
alaFcIntfEtunnelStatsTable
   alaFcIntfEtunnelStatsIfIndex
   alaFcIntfEtunnelStatsClear
```

clear fibre-channel sessions

Clears the specified sessions on all FC ports.

clear fibre-channel sessions {npiv-proxy | r-proxy | e-tunnel | all}

Syntax Definitions

npiv-proxy	Clears NP_Port proxy sessions.
r-proxy	Clears reverse NP_Port proxy sessions.
e-tunnel	Clears E-Tunnel (E2E Tunnel) sessions.
all	Clears all NP_Port proxy, reverse proxy, and E-Tunnel sessions.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Only the sessions associated with the specified parameter are cleared. For example, if the **npiv-proxy** parameter is used, only NPIV proxy sessions are cleared. All other session types remain active.
- When sessions are cleared on FC ports, the corresponding sessions on the FCoE ports are also cleared.

Examples

```
-> clear fibre-channel sessions npiv-proxy
-> clear fibre-channel sessions r-npiv
-> clear fibre-channel sessions e-tunnel
-> clear fibre-channel sessions all
```

Release History

Release 7.3.3; command introduced.

Related Commands

show fibre-channel sessions	Displays FC sessions.

MIB Objects

```
alaFcInfo
   alaFcConfigSessClear
```

clear fcoe statistics npiv

Clears N_Port proxy (NP_Port) statistics for FCoE interfaces or specific FCoE VLANs.

clear fcoe statistics npiv-proxy {interface | vlan [*vlan_id***[***vlan_id2***] | port** *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

interface	Clears statistics for all FCoE interfaces (ports and link aggregates).
*vlan_id***[***vlan_id2***]**	An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VLAN IDs (100-150).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **vlan** parameter to clear statistics for a specific FCoE VLAN ID.
- Use the **port** or **linkagg** parameters to clear statistics for a specific FCoE port or link aggregate ID.

Examples

```
-> clear fcoe statistics npiv-proxy interface
-> clear fcoe statistics npiv-proxy vlan 100
-> clear fcoe statistics npiv-proxy vlan 200-205
-> clear fcoe statistics npiv-proxy port 1/1
-> clear fcoe statistics npiv-proxy port 1/5-10
-> clear fcoe statistics npiv-proxy port 1/1/1
-> clear fcoe statistics npiv-proxy linkagg 10
```

Release History

Release 7.3.3; command introduced.

Related Commands

show fcoe statistics npiv-proxy Displays N_Port proxy statistics.

MIB Objects

```
alaFipsVlanTable
   alaFipsVlanStatsFnreClear
alaFipsIntfTable
   alaFipsIntfStatsFnreClear
```

clear fcoe statistics r-npiv

Clears F_Port proxy (reverse-NPIV) statistics for FCoE interfaces or specific FCoE VLANs.

clear fcoe statistics r-npiv {interface | vlan [*vlan_id***[***vlan_id2***] | port** *chassis/slot/port***[-***port2***]** | **linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

interface	Clears statistics for all FCoE interfaces (ports and link aggregates).
*vlan_id***[***vlan_id2***]**	An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VLAN IDs (100-150).
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **vlan** parameter to clear statistics for a specific FCoE VLAN ID.
- Use the **port** or **linkagg** parameters to clear statistics for a specific FCoE port or link aggregate ID.

Examples

```
-> clear fcoe statistics r-npiv interface
-> clear fcoe statistics r-npiv vlan 100
-> clear fcoe statistics r-npiv vlan 200-205
-> clear fcoe statistics r-npiv port 1/1
-> clear fcoe statistics r-npiv port 1/5-10
-> clear fcoe statistics r-npiv port 1/1/1
-> clear fcoe statistics r-npiv linkagg 10
```

Release History

Release 7.3.3; command introduced.

Related Commands

show fcoe statistics r-npiv	Displays F_Port proxy statistics.

MIB Objects

```
alaFipsVlanTable
   alaFipsVlanStatsFnreClear
alaFipsIntfTable
   alaFipsIntfStatsFnreClear
```

clear fcoe statistics e-tunnel

Clears E_Port proxy (E2E tunnel) statistics.

clear fcoe statistics e-tunnel [ve | te] {*tunnel_id***[-***tunnel_id***]}**

Syntax Definitions

ve	Clears VE_Port statistics**.**
te	Clears TE_Port statistics.
*tunnel_id***[-***tunnel_id***]**	The ID of an existing E2E tunnel. Use a hyphen to specify a range of tunnel IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **ve** parameter to clear only VE_Port statistics for the specified tunnel ID.
- Use the **te** parameter to clear only TE_Port statistics for the specified tunnel ID.

Examples

```
-> clear fcoe statistics e-tunnel 1
-> clear fcoe statistics e-tunnel ve 2
-> clear fcoe statistics e-tunnel te 2
```

Release History

Release 7.3.3; command introduced.

Related Commands

show fcoe statistics e-tunnel	Displays E_Port proxy (E2E tunnel) statistics.

MIB Objects

```
alaFipsEtunnelVePortStatsTable
   alaFipsEtunnelVePortStatsTunnelId
   alaFipsEtunnelVePortStatsClear
alaFipsEtunnelTePortStatsTable
   alaFipsEtunnelTePortStatsTunnelId
   alaFipsEtunnelTePortStatsClear
```

clear fcoe sessions

Clears the specified sessions on all FCoE ports.

clear fcoe sessions [fips | npiv-proxy | r-proxy | e-tunnel | all]

Syntax Definitions

fips	Clears FIP snooping sessions.
npiv-proxy	Clears NP_Port proxy sessions.
r-proxy	Clears reverse NP_Port proxy sessions.
e-tunnel	Clears E-Tunnel (E2E Tunnel) sessions.
all	Clears all FCoE, NP_Port proxy, reverse proxy, and E-Tunnel sessions.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When FIP snooping sessions are cleared, a clear virtual link (CVL) request is sent for all logged ENodes.
- When R-NPIV sessions are cleared, FIP FLOGO is sent to the FCF and FC FLOGO is sent to the HBA for each R-NPIV session created.
- Once sessions are cleared, NP_Ports will trigger a fabric login to the connected fabric.

Examples

```
-> clear fcoe sessions fips
-> clear fcoe sessions npiv-proxy
-> clear fcoe sessions r-npiv
-> clear fcoe sessions e-tunnel
-> clear fcoe sessions all
```

Release History

Release 7.3.3; command introduced.

Related Commands

show fcoe sessions	Displays the FCoE session information for the switch.

MIB Objects

```
alaFipsInfo
   alaFipsConfigSessClear
```

44 VXLAN Snooping Commands

The OmniSwitch Virtual eXtensible LAN (VXLAN) Snooping feature attempts to detect and identify VXLAN traffic by sampling packets to determine if they are VXLAN encapsulated packets. Once this type of traffic is identified, VXLAN Snooping collects and stores information about the flow in a database on the local switch. Additional configurable options for this feature include the ability to apply QoS policy list rules to the identified flow and SNMP trap generation.

A VXLAN segment is a Layer 2 overlay network through which devices can communicate. Traffic from such devices is encapsulated into VXLAN frames and then tunneled through the VXLAN segment. Using this implementation of VXLAN Snooping, an administrator can obtain more detailed information about the traffic flow through the overlay network.

Note. Throughout this chapter, the terms “VXLAN Snooping” and “VM Snooping” are interchangeable.

MIB information for the VXLAN Snooping commands is as follows:

Filename: ALCATEL-IND1-VM-SNOOPING-MIB.mib
Module: alaVMSnoopingMIB

A summary of the available commands is listed here:

vm-snooping admin-state

Configures the global status of the VXLAN Snooping process for the switch.

vm-snooping admin-state {enable | disable}

Syntax Definitions

enable	Enables VXLAN Snooping for the switch.
disable	Disables VXLAN Snooping for the switch.

Defaults

By default, VXLAN Snooping is disabled for the switch.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Enable VXLAN Snooping first before attempting any other VXLAN Snooping command. When enabled, the switch allocates resources for this feature. When disabled, switch resources are released for other purposes.
- This command enables or disables this feature on all VXLAN Snooping ports.

Examples

```
-> vm-snooping admin-state enable
-> vm-snooping admin-state disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the VXLAN Snooping configuration for the switch.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingAdminStatus
```

vm-snooping policy-mode

Configures the allocation of hardware resources for VXLAN Snooping. Use this command to change the policy lookup mode to basic or advanced and specify the number of policies reserved for VXLAN Snooping. In addition, an optional inner header parameter is available to specify if the header of the inner Ethernet frame is tagged or untagged.

vm-snooping policy-mode {basic | advance} [policy-resource {extended | default}] [inner-header {tagged | untagged | default}]

Syntax Definitions

basic	Reserves resources for VNI, VXLAN UDP port, inner source MAC address, and inner IPv4 source address policy conditions.
advance	For IPv4 packets, reserves resources for VNI, VXLAN UDP port, inner source MAC address, inner IPv4 source address, IP protocol, and Layer 4 source and destination port policy conditions. For IPv6 packets, reserves resources for VNI, VXLAN UDP port, inner source IPv6 address, Layer 4 source and destination port for policy conditions.
policy-resource extended	Doubles the amount of resources for VXLAN Snooping policies.
policy-resource default	Reserves the minimum amount of resources for VXLAN Snooping policies.
inner-header tagged	The header of the inner frame is tagged.
inner-header untagged	The header of the inner frame is untagged.
inner-header default	The header of the inner frame is either tagged or untagged (basic mode) or just tagged (advance mode).

Defaults

parameter	default
[basic | advance]	**basic**
[extended | default]	**default**

By default, the inner header option is set to the following values based on the current policy lookup mode:

- Basic mode—untagged and tagged header for the inner frame.
- Advanced mode—tagged header for the inner frame.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- To change the policy mode, globally disable VXLAN Snooping then make the changes and enable VXLAN Snooping again to apply the changes to the switch. This command is also allowed when the VXLAN Snooping feature is globally disabled.
- When the VXLAN Snooping policy mode is changed, all database and QoS entries are flushed.
- When the VXLAN policy mode is set to **basic**, any QoS policy rules with advanced mode policy conditions will not work. When the mode is set to **advance**, QoS policy rules with basic *and* advance policy conditions will work.
- When configuring the **inner-header** parameter for **basic** mode, specifying only tagged or only untagged may increase the number of policies allowed. In other words, specifying both tagged and untagged (the default) may reduce the number of policies allowed.
- When configuring the **inner-header** parameter for **advance** mode, specifying both tagged and untagged is not allowed. In this case, the **default** option sets the parameter to tagged.
- Other applications, such as QoS user policies, VLAN Stacking, Application Fingerprinting, DHCP Snooping, Open Flow, IP multicast, and FIP Snooping also use up system resources. Depending on which application comes first, other applications may not be able to get the required hardware resources.
- If the resources are increased by two times (**policy-resource extended**), then none of the above-mentioned applications can work simultaneously.
- Only one set of hardware resources are reserved for the VXLAN Snooping application when VXLAN Snooping is globally enabled.

Examples

```
-> vm-snooping admin-state disable
-> vm-snooping policy-mode basic policy-resource extended inner-header tagged
-> vm-snooping admin-state enable

-> vm-snooping admin-state disable
-> vm-snooping policy-mode advance policy-resource extended inner-header untagged
-> vm-snooping admin-state enable

-> vm-snooping admin-state disable
-> vm-snooping policy-mode basic inner-header default
-> vm-snooping policy-mode advance inner-header default
-> vm-snooping admin-state enable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the VXLAN Snooping configuration for the switch.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingPolicyMode
   alaVMSnoopingPolicyResource
   alaVMSnoopingVMTrafficTagged
```

vm-snooping trap

Enables or disables trap generation for the VXLAN Snooping feature.

vm-snooping trap {enable | disable}

Syntax Definitions

enable	Enables VXLAN Snooping trap generation.
disable	Disables VXLAN Snooping trap generation.

Defaults

By default, trap generation for this feature is disabled.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

A trap is generated when one of the following occurs:

- A new VXLAN database entry is learned or ages out.
- The usage of system resources allocated for VXLAN Snooping exceeds a configurable threshold value.

Examples

```
-> vm-snooping trap enable
-> vm-snooping trap disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

vm-snooping filtering-resource trap threshold	Configures the threshold value at which point the switch generates a trap to indicate that VXLAN Snooping has utilized the specified level of system resources.
show vm-snooping config	Displays the VXLAN Snooping status and configuration for the switch.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingTrapStatus
```

vm-snooping filtering-resource trap threshold

Configures the threshold value at which point the switch generates a trap to indicate that VXLAN Snooping has utilized the specified level of system resources.

vm-snooping filtering-resource trap threshold {*percentage* **| default}**

Syntax Definitions

percentage	The percentage of system resources used by VXLAN Snooping.
default	Sets the trap threshold value back to 80 percent (the default).

Defaults

By default, the filtering resource threshold is set to 80 percent.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

A trap is generated when the system resources used by VXLAN Snooping reach the specified threshold value.

Examples

```
-> vm-snooping filtering-resource trap threshold 50
-> vm-snooping filtering-resource trap threshold default
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the VXLAN Snooping status and configuration for the switch.
show vm-snooping filtering-resource	Displays the system resources used by VXLAN Snooping on a per-port basis.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingFilteringResourceTrapThreshold
```

vm-snooping sampling-rate

Configures the packets-per-second (pps) sampling rate for the VXLAN Snooping feature.

vm-snooping sampling-rate *pps*

Syntax Definitions

pps	The number of packets-per-second to sample on all VXLAN Snooping ports. The valid range is 1–1000.

Defaults

By default, the sampling rate is set to 1000 pps.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

The sampling rate value specified with this command is applied to every VXLAN Snooping port on the switch.

Examples

```
-> vm-snooping sampling-rate 500
-> vm-snooping sampling-rate 1000
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the VXLAN Snooping status and configuration for the switch.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingSamplingRate
```

vm-snooping aging-timer

Configures the aging time value for VXLAN packet flows learned in the VXLAN Snooping database on the local switch.

vm-snooping aging-timer *seconds*

Syntax Definitions

seconds	The number of seconds to wait before aging out a learned VM. The valid range is 60–86400 seconds.

Defaults

By default, the aging timer is set to 300 seconds.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Set this timer to zero to prevent the learned VMs from aging out.
- Note that an inactive VXLAN packet flow (no packets received for the flow) can take up to twice as long as the aging time value specified to be removed from the VXLAN Snooping database. For example, if an aging time of 300 seconds is specified, the database entry for the flow ages out any time between 300 and 600 seconds of inactivity.

Examples

```
-> vm-snooping aging-timer 100
-> vm-snooping aging-timer 300
-> vm-snooping aging-timer 0
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the VXLAN Snooping status and configuration for the switch.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingAgingTimer
```

vm-snooping vxlan udp-port

Configures additional UDP destination port numbers to look for when the switch inspects packets received on VXLAN Snooping ports. This value is used to identify encapsulated VXLAN packets.

vm-snooping vxlan udp-port {*udp_port_num***[-***udp_port_num2***}**

no vm-snooping vxlan udp-port {*udp_port_num***[-***udp_port_num2***}**

Syntax Definitions

*udp_port_num***[-***udp_port_num2*	The UDP destination port number. Use a hyphen to specify a range of port numbers. Do not specify a range that configures more than seven UDP ports.

Defaults

By default, the well-known UDP port number 4789 is used.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a UDP destination port number. Note that the default UDP port number of 4789 is not configurable, so it can not be removed with this command. Only port numbers that were added through this command can be removed.
- Avoid using the well-known UDP ports that are already reserved by IANA for other applications.
- Including the default UDP port number (4789), up to eight UDP ports are allowed. However, configuring multiple UDP ports may slow down the VXLAN Snooping process.
- Changing the UDP port number on the fly might stop the VXLAN traffic until the VXLAN Tunnel End Points (VTEPs) in the network are configured with the same destination UDP port.

Examples

```
-> vm-snooping vxlan udp-port 8472
-> no vm-snooping vxlan udp-port 8472
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the destination UDP port value that is used to identify VXLAN traffic.

MIB Objects

```
alaVMSnoopingUDPPortTable
      alaVMSnoopingUDPPortIndex
       alaVMSnoopingUDPRowStatus
```

vm-snooping static-policy rule

Configures a static QoS policy rule. When configured, QoS resources are automatically allocated for the specified rule even if there is no VXLAN packet flow that matches the rule conditions.

vm-snooping static-policy rule *rule_name* **[list** *list_name***]**

no vm-snooping static-policy rule *rule_name* **[list** *list_name***]**

Syntax Definitions

rule_name	The name of the policy rule (alphanumeric string up to 32 characters).
list_name	The name of the policy list (alphanumeric string up to 32 characters).

Defaults

parameter	default
list_name	"Default"

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a static VXLAN Snooping policy rule. If the rule is associated with a user-configured policy list (not the default list), then the list name must be specified as well to remove the static policy rule. If the rule is associated with the default list, then specifying a list name is not required to remove the static policy rule.
- The default policy list available in every switch has no name and is not configurable. All QoS policy rules are assigned to the default list unless the **no default-list** option of the **policy rule** command is used at the time the rule is created.

Examples

```
-> vm-snooping static-policy rule r1
-> vm-snooping static-policy rule r2 list l2
-> no vm-snooping static-policy rule r1
-> no vm-snooping static-policy rule r2 list l2
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping static-policy Displays the static policy configuration.

MIB Objects

```
alaVMSnoopingStaticPolicyTable
   alaVMSnoopingStaticPolicyRuleName
   alaVMSnoopingStaticPolicyListName
   alaVMSnoopingStaticPolicyRowStatus
```

vm-snooping logging-threshold

Configures the threshold value that determines how many entries for VXLAN packet flows and statistics are logged into a .csv file on the local switch.

vm-snooping logging-threshold number-of-flows {*flow_num* **| default}**

Syntax Definitions

flow_num	The number of VXLAN packet flows to log. The range is 1000–6000.
default	Sets the logging threshold value back to 5000 (the default).

Defaults

By default, the logging threshold value is set to 5000 packet flows.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Set the logging threshold value to zero to turn off the logging function.
- When the logging function is on, setting the VXLAN Snooping aging timer to 300 seconds is recommended. If the aging timer is set to zero, no logging occurs regardless of this threshold setting.
- The packet flows and hardware statistics are logged to the **vm_snoop_db_flow_rec.csv** file and the **vm_snoop_hw_stats_rec.csv** file in the **/flash/switch/bridge/vm_snoop/** directory on the local switch to maintain a packet flow history.
- When the number of records logged to the .csv files exceeds the logging threshold value, the corresponding files are renamed to **/flash/switch/bridge/vm_snoop/vm_snoop_db_flow_old_rec.csv** and to **/flash/switch/bridge/vm_snoop_hw_stats_old_rec.csv**.
- These files are accessed and used by Alcatel-Lucent Enterprise network management tools to provide management and visibility of the overlay network traffic.

Examples

```
-> vm-snooping logging-threshold number-of-flows 1000
-> vm-snooping logging-threshold number-of-flows 0
-> vm-snooping logging-threshold number-of-flows default
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the VXLAN Snooping status and configuration for the switch.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingLoggingThresholdFlows
```

vm-snooping port

Configures a switch port or link aggregate as a VXLAN Snooping interface. Once the interface is configured and enabled and VXLAN Snooping is enabled for the switch, IP packets received on the interface are sampled to determine if they contain the designated UDP destination port.

vm-snooping {port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]} [admin-state {enable | disable}]**

no vm-snooping {port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables the VXLAN Snooping administrative status on the port or link aggregate ID.
disable	Disables the VXLAN Snooping administrative status on the port or link aggregate ID

Defaults

By default, VXLAN Snooping is disabled on all switch ports and link aggregates.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to revert the VXLAN Snooping interface back to a regular switch port or link aggregate. This will clear the VXLAN Snooping configuration from the interface.
- Disabling the administrative status of a VXLAN Snooping interface does not remove the VXLAN Snooping configuration from the interface.
- Make sure the VXLAN Snooping feature is globally enabled for the switch to ensure that VXLAN Snooping ports will process VXLAN packets.
- VXLAN Snooping uses the sFlow mechanism to sample packets.

Examples

```
-> vm-snooping port 1/1/1
-> vm-snooping port 1/1/5-10
-> no vm-snooping port 1/1/1
-> no vm-snooping port 1/1/5-10
-> vm-snooping port 1/1/1 admin-state enable
-> vm-snooping port 1/1/5-10 admin-state enable
```

```
-> vm-snooping port 1/1/1 admin-state disable
-> vm-snooping port 1/1/5-10 admin-state disable

-> vm-snooping linkagg 1
-> vm-snooping linkagg 5-10
-> no vm-snooping linkagg 1
-> no vm-snooping linkagg 5-10
-> vm-snooping linkagg 1 admin-state enable
-> vm-snooping linkagg 5-10 admin-state enable
-> vm-snooping linkagg 1 admin-state disable
-> vm-snooping linkagg 5-10 admin-state disable
```

Release History

Release 7.3.4; command was introduced.

Related Commands

vm-snooping admin-state	Configures the global VXLAN Snooping status for the switch.
show vm-snooping port	Displays the VXLAN Snooping port configuration.

MIB Objects

```
alaVMSnoopingPortTable
   alaVMSnoopingPortIndex
   alaVMSnoopingPortAdminStatus
   alaVMSnoopingPortIsVNP
   alaVMSnoopingPortRowStatus
```

show vm-snooping config

Displays the global VXLAN Snooping status and configuration information for the switch.

show vm-snooping config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show vm-snooping config
VM-Snooping Status                          : Enable,
Trap                                        : Disable,
Trap-Threshold                              : 80,
Policy-Mode                                 : Basic
Policy-Resource                             : Default
VM Inner Header                             : Tagged and Untagged,
Aging-Timer                                 : 300 seconds,
UDP-Port(s)                                 : 4789,
Sampling-Rate                               : 1000
Logging-Threshold                           : 5000
Qos Allocation Status                       : Success
```

output definitions

VM-Snooping Status	The global administrative status of VXLAN Snooping for the switch (**Enabled** or **Disabled**). Configured through the **vm-snooping admin-state** command.
Trap	The status of SNMP trap generation for the switch (**Enabled** or **Disabled**). Configured through the **vm-snooping trap** command.
Trap-Threshold	The percentage of switch resources used that will trigger the switch to generate a trap. Configured through the **vm-snooping filtering-resource trap threshold** command.
Policy-Mode	The policy mode setting that designates switch resources for VXLAN Snooping. Configured through the **vm-snooping policy-mode** command.

output definitions (continued)

Policy Resource	Indicates the number of VXLAN Snooping policies allowed (**Default** or **Extended**). Configured through the **vm-snooping policy-mode** command.
VM Inner Header	Whether to check tagged and/or untagged VM traffic. Configured through the **vm-snooping policy-mode** command.
Aging-Timer	The number of seconds before a learned VM is aged out. Configured through the **vm-snooping aging-timer** command.
UDP-Port(s)	The UDP port numbers to snoop for VXLAN packets. Configured through the **vm-snooping vxlan udp-port** command.
Sampling-Rate	The number of packets-per-second (pps) to sample. Configured through the **vm-snooping sampling-rate** command.
Logging-Threshold	The number of VXLAN packet flow entries and statistics logged to a .csv file on the local switch.
Qos Allocation Status	The status of QoS resource allocation (**Success**, **inProgress**, or **Failed**). This field is blank when VXLAN Snooping is disabled.

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping port	Displays the VXLAN Snooping port configuration.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingAdminStatus
   alaVMSnoopingPolicyMode
   alaVMSnoopingPolicyResource
   alaVMSnoopingVMTrafficTagged
   alaVMSnoopingTrapStatus
   alaVMSnoopingFilteringResourceTrapThreshold
   alaVMSnoopingAgingTimer
   alaVMSnoopingSamplingRate
   alaVMSnoopingLoggingThresholdFlows
   alaVMSnoopingQosAllocationStatus
alaVMSnoopingUdpPortTable
   alaVMSnoopingUdpPortIndex
   alaVMSnoopingUdpRowStatus
```

show vm-snooping port

Displays the VXLAN Snooping port configuration for the switch.

show vm-snooping port

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **port** and **linkagg** parameters to display information for a specific port or link aggregate.
- The display output also indicates whether or not the VXLAN Snooping port is a virtual machine network profile (vNP) port.

Examples

```
-> show vm-snooping port
Port    VM-Snooping   vNP
-------+------------+--------
1/2/1   Enable        Yes
1/2/2   Enable        No
1/2/2   Enable        Yes
1/2/2   Enable        Yes
0/12    Disable       No
```

output definitions

Port	The slot/port or link aggregate ID of the VXLAN Snooping interface. A “0” slot number indicates that the interface is a link aggregate.
VM-Snooping	The administrative status (**Enable** or **Disable**) of VXLAN Snooping on the port or link aggregate. Configured through the **vm-snooping port** command.
vNP	Whether the port is also a vNP port (**Yes** or **No**).

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the VXLAN Snooping status and configuration for the switch.

MIB Objects

```
alaVMSnoopingPortTable
   alaVMSnoopingPortIndex
   alaVMSnoopingPortAdminStatus
   alaVMSnoopingPortIsVNP
   alaVMSnoopingPortRowStatus
```

show vm-snooping database

Displays VXLAN Snooping database entries. When a VXLAN packet is detected and the packet contains the designated UDP destination port, VXLAN Snooping creates an entry in the local switch database to identify and track the VXLAN packet flow.

show vm-snooping database [vxlan udp-port *udp_port_num* **| vtep-ip** *ip_address* **| vni** *vxlan_id* **| vm-src-mac** *mac_address* **| vm-ip** *ip_address***] [detail] [port** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]] [detail]**

Syntax Definitions

udp_port_num	The UDP destination port number used to identify VXLAN traffic.
vtep-ip *ip_address*	The IP address of the VXLAN Tunnel End Point (VTEP). This is the Loopback0 interface address on the OmniSwitch.
vxlan_id	The VXLAN Network Identifier (VNI) for the VXLAN segment on which the VM was learned.
mac_address	The source MAC address of a VM.
vm-ip *ip_address*	The source IP address of a VM.
detail	Displays additional information about the classified traffic flow.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, all database entries are displayed.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **port** and **linkagg** parameters to display information for a specific port or link aggregate.
- Each database entry is subject to a VXLAN Snooping aging period. If the database fills up, older entries are aged out before the limit (fast aging).
- When a database entry is removed due to regular aging or fast aging conditions, any corresponding QoS is also removed for that flow.

Examples

```
-> show vm-snooping database
Total number of VM Flows: 15

        VXLAN                VM          VM         VM
Port    PORT   VNI         SRC MAC       VLAN      SRC IP
------+------+--------+----------------+-----+-----------------------------------
1/1/3  4789   2000     00:12:01:00:00:01    -  200.200.200.1
1/1/3  4789   2001     00:12:01:00:00:02    -  200.200.201.1
1/1/3  4789   2002     00:12:01:00:00:03    -  200.200.202.1
1/1/3  4789   2003     00:12:01:00:00:04    -  200.200.203.1
1/1/3  4789   2004     00:12:01:00:00:05    -  200.200.204.1
1/1/3  4789   1234     00:00:04:00:00:00    -  2.0.0.0
1/1/3  4789   1234     00:00:04:00:00:01    -  2.0.0.1
1/1/3  4789   1234     00:00:04:00:00:02    -  2.0.0.2
1/1/3  4789   1234     00:00:04:00:00:03    -  2.0.0.3
1/1/3  4789   1234     00:00:04:00:00:04    -  2.0.0.4
1/2/2  4789   43       00:00:00:88:00:01 8     88.0.0.1
1/2/2  4789   43       00:00:00:88:00:02 8     88.0.0.2
1/2/2  4789   43       00:00:00:88:00:03 8     88.0.0.3
1/2/2  4789   43       00:00:00:88:00:04 8     88.0.0.4
1/2/2  4789   43       00:00:00:88:00:05 8     88.0.0.5

-> show vm-snooping database port 1/2/2
Total number of VM Flows: 5

        VXLAN                VM          VM         VM
Port    PORT   VNI         SRC MAC       VLAN      SRC IP
------+------+--------+----------------+-----+-----------------------------------
1/2/2  4789   43       00:00:00:88:00:01 8     88.0.0.1
1/2/2  4789   43       00:00:00:88:00:02 8     88.0.0.2
1/2/2  4789   43       00:00:00:88:00:03 8     88.0.0.3
1/2/2  4789   43       00:00:00:88:00:04 8     88.0.0.4
1/2/2  4789   43       00:00:00:88:00:05 8     88.0.0.5

-> show vm-snooping database vni 1234
Total number of VM Flows: 5

        VXLAN                VM          VM         VM
Port    PORT   VNI         SRC MAC       VLAN      SRC IP
------+------+--------+----------------+-----+-----------------------------------
1/1/3  4789   1234     00:00:04:00:00:00    -  2.0.0.0
1/1/3  4789   1234     00:00:04:00:00:01    -  2.0.0.1
1/1/3  4789   1234     00:00:04:00:00:02    -  2.0.0.2
1/1/3  4789   1234     00:00:04:00:00:03    -  2.0.0.3
1/1/3  4789   1234     00:00:04:00:00:04    -  2.0.0.4
```

output definitions

Port	The slot/port or link aggregate ID of the VXLAN Snooping interface. A “0” slot number indicates a link aggregate.
VXLAN Port	The UDP port for the VXLAN segment.
VNI	The VXLAN Network ID (VNI) for the VXLAN segment on which the VM was learned.
VM SRC MAC	The source MAC address of the VM.

output definitions (continued)

VM VLAN	The VLAN ID tag for the VM packet.
VM SRC IP	The source IP address of the VM.

```
-> show vm-snooping database detail
Total number of VM Flows: 2

Port:                        1/1/3,
VTEP SRC IP:                 100.0.1.1,
VTEP DEST IP:                100.0.1.2,
VTEP VLAN:                   100,
VXLAN VNI:                   2000,
VXLAN PORT:                  4789,
VM SRC MAC:                  00:12:01:00:00:01,
VM DEST MAC:                 00:14:01:00:00:01,
VM VLAN:                     UnTagged,
VM SRC IP/PORT:              200.200.200.1/1,
VM DEST IP/PORT:             200.200.200.2/515,
VM IP PROTO:                 61,
POLICY RULE:                 r1,
POLICY LIST:                 Default,
SAMPLED PKTS                 170,
LEARNED TIME                 Mon Dec 15 11:58:50 2014

Port:                        1/1/3,
VTEP SRC IP:                 100.0.2.1,
VTEP DEST IP:                100.0.2.2,
VTEP VLAN:                   100,
VXLAN VNI:                   2001,
VXLAN PORT:                  4789,
VM SRC MAC:                  00:12:01:00:00:02,
VM DEST MAC:                 00:14:01:00:00:02,
VM VLAN:                     UnTagged,
VM SRC IP/PORT:              200.200.201.1/1,
VM DEST IP/PORT:             200.200.201.2/515,
VM IP PROTO:                 61,
POLICY RULE:                 r2,
POLICY LIST:                 Default,
SAMPLED PKTS                 177,
LEARNED TIME                 Mon Dec 15 11:58:50 2014
```

Port	The slot/port or link aggregate ID of the VXLAN Snooping interface. A “0” slot number indicates a link aggregate.
VTEP SRC IP	The source IP network address for the VTEP.
VTEP DST IP	The destination IP network address for the VTEP.
VTEP VLAN	The VLAN ID associated with the VTEP.
VXLAN VNI	The VNI for the VXLAN segment on which the VM was learned.
VXLAN Port	The UDP port for the VXLAN segment.
VM SRC MAC	The source MAC address for the VM.
VM DEST MAC	The destination MAC address for the VM.
VM VLAN	The VLAN on which the VM is learned and forwarded.

VM SRC IP/PORT	The source IP address of the VM.
VM DEST IP/PORT	The destination IP address of the VM.
VM IP PROTO	The IP protocol version for the VM.
POLICY RULE	The name of the QoS policy rule applied to the VM flow.
POLICY LIST	The name of the QoS policy list applied to the VM flow.
SAMPLED PKTS	The number of packets sampled for this flow.
LEARNED TIME	The date and time the flow entry was learned.

Release History

Release 7.3.4; command was introduced.

Related Commands

clear vm-snooping database	Clears the local database entries for each virtual machine (VM) flow.
show vm-snooping config	Displays the VXLAN Snooping configuration for the switch.
show vm-snooping port	Displays the VXLAN Snooping port configuration.

MIB Objects

```
alaVMSnoopingDBTable
   alaVMSnoopingDBFlowId
   alaVMSnoopingDBIfIndex
   alaVMSnoopingDBVxlanUdpDestPort
   alaVMSnoopingDBVni
   alaVMSnoopingDBVtepVlan
   alaVMSnoopingDBVtepSrcIpAddrType
   alaVMSnoopingDBVtepSrcIpAddr
   alaVMSnoopingDBVtepDestIpAddrType
   alaVMSnoopingDBVtepDestIpAddr
   alaVMSnoopingDBInnerSrcMacAddr
   alaVMSnoopingDBInnerDestMacAddr
   alaVMSnoopingDBInnerVlan
   alaVMSnoopingDBInnerSrcIpAddrType
   alaVMSnoopingDBInnerSrcIpAddr
   alaVMSnoopingDBInnerDestIpAddrType
   alaVMSnoopingDBInnerDestIpAddr
   alaVMSnoopingDBVInnerL4SrcPort
   alaVMSnoopingDBVInnerL4DestPort
   alaVMSnoopingDBVInnerIPProtocol
   alaVMSnoopingDBPolicyRule
   alaVMSnoopingDBPolicyList
   alaVMSnoopingDBSamplingStatsPackets
```

clear vm-snooping database

Clears the local database entries for each virtual machine (VM) flow.

clear vm-snooping database [port *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, all database entries are cleared for all VXLAN Snooping ports and link aggregates.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **port** and **linkagg** parameters to clear database entries for a specific port or link aggregate.

Examples

```
-> clear vm-snooping database
-> clear vm-snooping database port 3/1/1
-> clear vm-snooping database linkagg 10
```

Release History

Release 7.3.4; command introduced.

Related Commands

show vm-snooping database	Displays the contents of the VXLAN Snooping database.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingClearAllData
 alaVMSnoopingDBTable
   alaVMSnoopingDBClearStats
```

show vm-snooping virtual-machines

Displays the port, source MAC address, and VLAN associated with Virtual Machines (VMs) discovered through the VXLAN Snooping process.

show vm-snooping virtual-machines

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

The output display of this command shows the port, source MAC address, and VLAN associated with each VM learned through the VXLAN Snooping process.

Examples

```
-> show vm-snooping virtual-machines
Port       SRC MAC       VLAN
------+-----------------+-----+
1/1/2  00:00:00:88:00:01  -
1/1/2  00:00:00:88:00:02  -
1/1/2  00:00:00:88:00:03  -
1/1/2  00:00:00:88:00:04  -
1/1/2  00:00:00:88:00:05  -
```

output definitions

Port	The slot/port or link aggregate ID of the VXLAN Snooping interface. A “0” slot number indicates a link aggregate.
SRC MAC	The source MAC address of the VM.
VLAN	The VLAN on which the VM is learned and forwarded.

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config	Displays the VXLAN Snooping configuration for the switch.
show vm-snooping database	Displays the contents of the local VXLAN Snooping database.

MIB Objects

```
alaVMSnoopingLearntVMTable
   alaVMSnoopingLearntVMIfIndex,
   alaVMSnoopingLearntVMSrcMac,
   alaVMSnoopingLearntVMVlanId
```

show vm-snooping filtering-resource

Displays the amount of switch resources available for and used by QoS policies that contain VXLAN conditions.

show vm-snooping filtering-resource

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- VXLAN Snooping uses the amount of resources used to calculate the percentage of switch resources used and then determine if that percentage exceeds the value set for the filtering trap threshold. An SNMP trap is generated when the percentage used meets or exceeds the trap threshold value.
- The output display of this command shows the percentage of switch resources used by VXLAN policies on a per-slot basis.

Examples

```
-> show vm-snooping filtering-resource
Total Filtering Resources     :256,
Chassis/Slot    Filtering Resources Used
--------------+---------------------------
  1/SLOT-1       0
  2/SLOT-1       0
```

Release History

Release 7.3.4; command was introduced.

Related Commands

vm-snooping filtering-resource trap threshold	Configures the trap threshold value for system resources used by VXLAN Snooping.
show vm-snooping config	Displays the VXLAN Snooping status and configuration for the switch.

MIB Objects

```
alaVMSnoopingFilterResourceTable
   alaVMSnoopingFilterResourceChassisId
   alaVMSnoopingFilterResourceSlotNum
   alaVMSnoopingFilterResourceMax
   alaVMSnoopingFilterResourceUsed
```

show vm-snooping statistics

Displays statistics for each VXLAN packet flow on a VXLAN Snooping port or link aggregate.

show vm-snooping statistics [hardware | sampling] [port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]]**

Syntax Definitions

hardware	Displays the VXLAN policy rule and list and the number of packets and bytes on which the policy rule was applied.
sampling	Displays the number of VXLAN packets that were sampled for a specific flow.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, statistics are displayed for all VXLAN Snooping ports and link aggregates.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **port** and **linkagg** parameters to display information for a specific port or link aggregate.

Examples

```
-> show vm-snooping statistics
Total number of Hardware Statistics: 0

Policy Rule                 Policy List        Number of pkts       Number of Bytes
---------------------------+------------------+--------------------+--------------+
Total number of Sampling Statistics: 1

        VXLAN    VXLAN       VM               VM          Pkts
Port   UDP PORT   VNI       SRC MAC          SRC IP
-----+---------+------+------------------+--------------+---------+
2/1/2      4789     43 00:00:00:88:00:01         88.0.0.1    15

-> show vm-snooping statistics sampling
Total number of Sampling Statistics: 1

        VXLAN    VXLAN       VM               VM          Pkts
Port   UDP PORT   VNI       SRC MAC          SRC IP
-----+---------+------+------------------+--------------+---------+
1/1/2      4789     43 00:00:00:99:00:01         99.0.0.1    10
```

```
-> show vm-snooping statistics hardware
Total number of Hardware Statistics: 1

Policy Rule                 Policy List        Number of pkts       Number of Bytes
----------------------------+------------------+--------------------+--------------+
r1                          Default            497                  45724
```

Release History

Release 7.3.4; command introduced.

Related Commands

clear vm-snooping statistics Clears VXLAN Snooping statistics.

MIB Objects

```
alaVMSnoopingHardwareStatsTable
   alaVMSnoopingHardwareStatsPolicylist
   alaVMSnoopingHardwareStatsPolicyrule
   alaVMSnoopingHardwareStatsNumOfPackets
   alaVMSnoopingHardwareStatsNumOfBytes
```

show vm-snooping static-policy

Displays the static QoS policy rule configuration for VXLAN Snooping.

show vm-snooping static-policy

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When a static policy rule is configured for VXLAN Snooping, QoS resources are automatically allocated for the specified rule even if there is no VXLAN packet flow that matches the rule conditions.
- If the static policy rule was created with a user-configured policy list (not the default list), then the list name appears in the “Policy List” field. However, if the static policy rule was created without specifying a policy list name, then the “Default” list name appears in the “Policy List” field.

Examples

```
-> show vm-snooping static-policy
Total number of Static-Policy: 5

Policy Rule                      Policy List
---------------------------------+---------------------------------
r0                                Default
r1                                Default
r2                                L1
r2                                l3
r2                                Default
```

output definitions

Policy Rule	The name of the QoS policy rule that was specified when the static policy rule was created.
Policy List	The name of the QoS policy list associated with the static policy rule.

Release History

Release 7.3.4; command was introduced.

Related Commands

vm-snooping static-policy rule Configures a VXLAN Snooping static policy rule.

MIB Objects

```
alaVMSnoopingStaticPolicyTable
   alaVMSnoopingStaticPolicyRuleName
   alaVMSnoopingStaticPolicyListName
   alaVMSnoopingStaticPolicyRowStatus
```

clear vm-snooping statistics

Clears the collected statistics for each VXLAN packet flow on a VXLAN Snooping port or link aggregate.

clear vm-snooping statistics [sampling [port *chassis/slot/port***[-***port2***] | linkagg** *agg_id***[-***agg_id2***]]] [hardware]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
*agg_id***[-***agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, statistics are cleared on all VXLAN Snooping ports and link aggregates.

Platforms Supported

OmniSwitch 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **port** and **linkagg** parameters to clear statistics for a specific port or link aggregate.

Examples

```
-> clear vm-snooping statistics
-> clear vm-snooping statistics sampling port 3/1/1
-> clear vm-snooping statistics sampling linkagg 10
-> clear vm-snooping statistics hardware
```

Release History

Release 7.3.4; command introduced.

Related Commands

show vm-snooping statistics	Displays VXLAN Snooping statistics.

MIB Objects

```
alaVMSnoopingConfig
   alaVMSnoopingClearAllData
alaVMSnoopingSamplingStatsTable
   alaVMSnoopingSamplingStatsClear
```

45 Port Mapping Commands

Port Mapping is a security feature that controls communication between peer users. Each session comprises of a session ID and a set of user ports and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate through network ports. In a port mapping session with user port set A and network port set B, ports in set A can communicate with ports in set B only. If set B is empty, the ports in set A can communicate with the rest of the ports in the system.

A port mapping session can be configured in a unidirectional or bidirectional mode. In the unidirectional mode, the network ports can communicate with each other within the same session. In the bidirectional mode, the network ports cannot communicate with each other. Network ports of a unidirectional port mapping session can be shared with other unidirectional sessions, but cannot be shared with any session that is configured in bidirectional mode. Network ports of different sessions can communicate with each other.

MIB information for the Port Mapping commands is as follows:

Filename: ALCATEL-IND1-PORT-MAPPING.mib
Module: alcatelIND1PortMappingMIB

A summary of the available commands is listed here:

port-mapping user-port network-port
port-mapping (configures port mapping status and direction)
port-mapping unidirectional bidirectional
port-mapping unknown-unicast-flooding
port-mapping dynamic-proxy-arp
show port-mapping status
show port-mapping

port-mapping user-port network-port

Creates a port mapping session with the user ports, network ports, or both user ports and network ports. Use the **no** form of the command to delete ports or a link aggregate group from a session.

port-mapping *session_id* **[user-port {slot** *chassis/slot* **|** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***}] [network-port {slot** *chassis/slot* **|** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***}]**

no port-mapping *session_id* **[user-port {slot** *chassis/slot* **|** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***}] [network-port {slot** *chassis/slot* **|** *chassis/slot/port***[**-*port2***] | linkagg** *agg_id***}]**

Syntax Definitions

session_id	The port mapping session ID.
user-port	Specifies a user port of the mapping session.
network-port	Specifies a network port of the mapping session.
chassis	The chassis identifier.
slot	The slot number to be assigned to the mapping session.
*slot/port***[**-*port2***]**	The slot and port number to assign to the mapping session. Use a hyphen to specify a range of ports (1/5-10).
agg_id	The link aggregate ID number to assign to the mapping session.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- User ports that are part of one session cannot communicate with each other. The user ports can communicate only through network ports of the session to the other elements of the system.
- User ports can be part of only one port mapping session.
- An aggregable port of a link aggregation group cannot be a mapped port and a mapped port cannot be an aggregable port of a link aggregation group.
- A mirrored port cannot be a mapped port and a mapped port cannot be a mirrored port.

Examples

```
-> port-mapping 3 user-port 2/3 network-port 6/4
-> port-mapping 4 user-port 2/5-8
-> port-mapping 5 user-port 2/3 network-port slot 3
-> no port-mapping 5 user-port 2/3
-> no port-mapping 6 network-port linkagg 7
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-mapping	Enables, disables, or deletes a port mapping session.
port-mapping unidirectional bidirectional	Configures the direction of a port mapping session.
port-mapping unknown-unicast-flooding	Enables or disables flooding of unknown unicast traffic from all ports to user ports for a particular session.
show port-mapping	Displays the configuration of one or more port mapping sessions.

MIB Objects

```
PortMappingSessionTable
   pmapSessionNumber
portMappingTable
   pmapPortIfindex
   pmapPortType
```

port-mapping

Enables, disables, or deletes a port mapping session.

port-mapping *session_id* **{enable | disable}**

no port-mapping *session_id*

Syntax Definitions

session_id	The port mapping session ID.
enable	Enables a port mapping session.
disable	Disables a port mapping session.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To be enabled, a session should have a minimum of two ports.

Examples

```
-> port-mapping 3 enable
-> port-mapping 4 disable
-> no port-mapping 5
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports, or both.
port-mapping unidirectional bidirectional	Configures the direction of a port mapping session.
show port-mapping status	Displays the status of one or more port mapping sessions.
show port-mapping	Displays the configuration of one or more port mapping sessions.

MIB Objects

```
PortMappingSessionTable
   pmapSessionNumber
   pmapSessionStatus
```

port-mapping unidirectional bidirectional

Configures the direction of a port mapping session.

port-mapping *session_id* **[unidirectional | bidirectional]**

Syntax Definitions

session_id	The port mapping session ID.
unidirectional	Specifies unidirectional port mapping.
bidirectional	Specifies bidirectional port mapping.

Defaults

parameter	default
enable | disable	**enable**
unidirectional | bidirectional	**bidirectional**

Platform Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

- In the bidirectional mode, the network ports of a session cannot communicate with each other. Also, the network ports of that session cannot be a part of a network port set of another session.
- In the unidirectional mode, the network ports of a session can communicate with each other. Also, the network ports of that session can be part of a network port set of another session that is in the unidirectional mode.
- To change the directional mode of an active session with network ports, delete the network ports of the session, change the direction, and recreate the network ports.

Examples

```
-> port-mapping 5 enable unidirectional
-> port-mapping 5 disable unidirectional
-> port-mapping 6 enable bidirectional
-> port-mapping 5 disable bidirectional
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports or both.
port-mapping	Enables, disables, or deletes a port mapping session.
show port-mapping	Displays the configuration of one or more port mapping sessions.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
   PmapSessionDirection
```

port-mapping unknown-unicast-flooding

Enables or disables flooding of unicast traffic from all the switch ports to the user ports related to a particular session.

port-mapping *session_id* **unknown-unicast-flooding {enable | disable}**

Syntax Definitions

session_id	The port mapping session ID.
enable	Enables the flooding of unknown unicast traffic from all ports to the user ports for a particular session.
disable	Disables the flooding of unknown unicast traffic from all ports to the user ports for a particular session.

Defaults

parameter	default
enable | disable	**enable**

Platform Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

- Configuring unknown unicast flooding creates a new port mapping session if there is no existing session.
- When a link aggregate is configured as a user port, the unknown unicast flooding configuration is applied to all the member ports of the aggregate.

Examples

```
-> port-mapping 1 unknown-unicast-flooding enable
-> port-mapping 2 unknown-unicast-flooding disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports or both.
port-mapping	Enables, disables, or deletes a port mapping session.
show port-mapping	Displays the configuration of one or more port mapping sessions.
show port-mapping status	Displays the status of one or more port mapping sessions.

MIB Objects

```
portMappingSessionTable
   pmapSessionUnknownUnicastFloodStatus
```

port-mapping dynamic-proxy-arp

Enables or disables the dynamic proxy ARP functionality for the port mapping session.

port-mapping *session_id* **dynamic-proxy-arp {enable | disable}**

Syntax Definitions

session_id	The port mapping session for which the dynamic proxy ARP status is enabled or disabled.
enable	Enables the dynamic proxy ARP status.
disable	Disables the dynamic proxy ARP status.

Defaults

parameter	default
enable | disable	**disable**

Platform Supported

OmniSwitch 6860, 6865

Usage Guidelines

- Clients must be connected to the user-ports and the head end routers connected to the network-ports of the port mapping session for dynamic proxy ARP to function properly.
- DHCP snooping must be enabled for dynamic proxy ARP to function.
- Using dynamic proxy ARP in conjunction with DHCP snooping allows for the configuration of the MAC Forced Forwarding feature.

Examples

```
-> port-mapping 1 dynamic-proxy-arp enable
-> port-mapping 1 dynamic-proxy-arp disable
```

Release History

Release 8.6R1; command was introduced.

Related Commands

port-mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports or both.
port-mapping	Enables, disables, or deletes a port mapping session.
show port-mapping	Displays the configuration of one or more port mapping session.
show port-mapping status	Displays the status of one or more port mapping session.

MIB Objects

```
portMappingSessionTable
   pmapSessionDynProxyARP
```

show port-mapping status

Displays the status of one or more port mapping sessions.

show port-mapping [*session_id***] status**

Syntax definitions

session_id	The port mapping session ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If you do not specify the port mapping session ID, then the status of all the port mapping sessions are displayed.

Examples

```
-> show port-mapping status

SessionID       Direction       Status          Unknown Unicast    DPA Status
------------+-----------------+--------------+------------------+--------------
     1           bi            disable         flood              enable
     1           bi            enable          drop               disable
     2           bi            disable         flood              disable
```

output definitions

SessionID	Displays the port mapping session ID.
Direction	Displays the direction of a port mapping session.
Status	Displays status of a port mapping session.
Unknown Unicast	Whether unknown unicast traffic is dropped or flooded from all the switch ports to the user ports related to the port mapping session
DPA Status	Displays the status of Dynamic Proxy ARP for the port mapping session. *This functionality is supported only on the OmniSwitch 6465 and OmniSwitch 6865*.

Release History

Release 7.1.1; command introduced.
Release 8.6R1; “DPA Status” field added.

Related Commands

port-mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports, or both.
port-mapping	Enables, disables, or deletes a port mapping session.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
   PmapSessionDirection
   pmapSessionStatus
   pmapSessionUnknownUnicastFloodStatus
   pmapSessionDynProxyARP
```

show port-mapping

Displays the configuration of one or more port mapping sessions.

show port-mapping [*session_id***]**

Syntax Definitions

session_id	The port mapping session ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If you do not specify the port mapping session ID, then the user port and network port information are displayed for all the port mapping sessions active on the switch.

Examples

```
-> show port-mapping 3

SessionID       USR-PORT        NETWORK-PORT
----------+---------------+------------------
     1           1/2               1/3
     1           1/6
     1           1/7
```

output definitions

SessionID	Displays the port mapping session ID.
USR-PORT	Displays the set of user ports of a port mapping session.
NETWORK-PORT	Displays the set of network ports of a port mapping session.

Release History

Release 7.1.1; command introduced.

Related Commands

port-mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports, or both.
port-mapping	Enables, disables, or deletes a port mapping session.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
PortMappingTable
   pmapPortIfindex
   pmapPortType
```

46 Learned Port Security Commands

Learned Port Security (LPS) provides a mechanism for controlling network device communication on one or more switch ports. Configurable LPS parameters allow the user to restrict source learning on a port to:

- A maximum number of learned source MAC addresses.
- A specific amount of time in which source MAC addresses are learned.
- An individual learned source MAC address.
- A range of learned source MAC addresses.

This chapter includes descriptions of the CLI commands used to define LPS parameters and display information about the current LPS configuration.

MIB information for Learned Port Security commands is as follows:

Filename: ALCATEL-IND1-LPS-MIB.mib
Module: alcatelIND1LearnedPortSecurityMIB

A summary of the available commands is listed here:

port-security

Enables or disables Learned Port Security (LPS) on the switch port(s). When LPS is enabled, only devices that have a source MAC address that complies with LPS restrictions are learned on the port(s).

port-security {port *chassis/slot/port***[-***port2***] | chassis} [admin-state {enable | disable | locked}]**

no port-security port *chassis/slot/port***[-***port2***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
chassis	Specifies all LPS ports.
enable	Administratively enables LPS on the specified port(s).
disable	Administratively disables LPS on the specified port(s). All bridged and filtered MAC addresses are cleared, but the static MAC address and LPS configuration for the port is retained. Learning is unrestricted.
locked	Administratively disables all learning on the port. Existing MAC addresses are retained but no additional learning of addresses, except for static MAC addresses, is allowed.

Defaults

By default, LPS functionality is disabled on all ports.

The following default value applies if the **admin-state** parameter is *not* specified with this command:

parameter	default
admin-state	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove the LPS configuration from the specified port *and* clear all MAC addresses learned on the port. Note that the **chassis** parameter is not supported when using the **no** form of this command.
- The **admin-state disable** option disables LPS on the port but does not clear the LPS configuration.
- Use the **chassis** parameter to administratively disable or enable all active LPS ports with one command. This option does not apply to ports on which LPS was not previously enabled.
- LPS is supported on Ethernet fixed and 802.1Q-tagged ports. However, LPS is *not* supported on ports that are configured as service access ports.

- LPS is not supported on link aggregates, 802.1Q tagged (trunked) link aggregates, or link aggregate member ports.
- Note that when LPS is enabled on an active port, all MAC addresses previously learned on that port are cleared from the source learning MAC address table.
- LPS is also supported on ports that have Universal Network Profile (UNP) functionality enabled, with the following conditions:
  - When LPS is enabled or disabled on a UNP bridge port (LPS is not supported on UNP access ports), MAC addresses already learned on that port are flushed.
  - UNP authentication and classification is applied first, then LPS rules.
  - If UNP classifies a MAC address as forwarding but LPS learns the address as filtering, an untagged packet will show as filtering in the default VLAN for the port and a tagged packet MAC will show as filtering in the specific tagged VLAN.
  - When a MAC address is filtered by LPS, the **show unp user status** command will display “LPS-B” as the profile classification source for that MAC address.
- LPS allows for the configuration of the following source MAC address learning restrictions:
  - A source learning time limit window to specify the length of time learning is allowed on a port.
  - A maximum number of bridged and filtered MAC addresses allowed on a specific port
  - A list of MAC addresses (individual or range of addresses) allowed on a port.
  - How a port handles traffic that is unauthorized.

Examples

```
-> port-security port 4/8 admin-state enable
-> port-security port 2/1-10 admin-state enable
-> port-security chassis admin-state disable
-> no port-security port 1/1-12
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security learning-window	Configures the amount of time, in minutes, to allow source learning on all LPS ports.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port(s).

MIB Objects

```
learnedPortSecurityTable
   lpsAdminStatus
```

port-security learning-window

Configures the amount of time, in minutes, to allow source learning on all LPS ports. This LPS parameter applies to the entire switch, so when the time limit expires, source learning of *new* MAC addresses is stopped on all LPS ports. Only authorized MAC addresses are allowed to be associated on LPS ports after this timer expires. This command also enables or disables the conversion of dynamic MAC addresses to static MAC addresses on LPS ports.

port-security learning-window *minutes* **[convert-to-static {enable | disable}] [no-aging {enable | disable}] [mac-move {enable | disable}] [learn-as-static {enable | disable}] [boot-up {enable | disable}]**

no port-security learning-window

Syntax Definitions

minutes	The number of minutes during which LPS allows source learning across all LPS ports. This amount of time defines the LPS learning window. The valid range is 0–2880. When this value is set to zero, the learning window time is set to infinity (no source learning time restriction on LPS ports).
convert-to-static enable	Enables the **convert-to-static** option for the learning window. Dynamically learned bridged (not filtered) MAC addresses are automatically converted to static addresses when the learning window closes. This option is automatically disabled when the LPS learning window is set to infinity (zero).
convert-to-static disable	Disables the **convert-to-static** option for the learning window. Dynamically learned bridged MAC addresses are not converted to static addresses and will start to age out when the learning window closes.
no-aging enable	Enables the **no-aging** option for the learning window. Dynamically learned bridged MAC addresses are learned as *pseudo-static* MACs, which do not age out but are not saved in the switch configuration. MAC movement is not allowed for pseudo-static MAC addresses unless the **mac-move** option is also enabled.
no-aging disable	Disables the **no-aging** option for the learning window. MAC addresses are learned as dynamic addresses that will age out.
mac-move enable	Enables the **mac-move** option. Allows a pseudo-static MAC address to move to a different port in the same VLAN without getting dropped. The **mac-move** option is used with the **no-aging** option to allow MAC movement for pseudo-static MAC addresses.
mac-move disable	Disables the **mac-move** option. If the **no-aging** option is enabled, MAC movement for pseudo-static MAC addresses is not allowed. Frames from a duplicate pseudo-static MAC address are dropped.
learn-as-static enable	Enables the **learn-as-static** option for the learning window. Dynamically learned bridged MAC addresses are converted to permanent static MAC addresses during the learning window time (even if the **convert-to-static** option is disabled). MAC movement is allowed for the permanent static MAC addresses. This option and the **no-aging** option are mutually exclusive.

learn-as-static disable	Disables the **learn-as-static** option for the learning window. Dynamically learned bridged MAC addresses are not converted to permanent static MAC addresses during the learning window time.
boot-up enable	Enables the automatic start of the LPS learning window timer when the switch restarts.
boot-up disable	Disables the automatic start of the LPS learning window timer when the switch restarts.

Defaults

By default, the LPS source learning time limit is not set for the switch; the learning window defaults to infinity (source learning is not limited to a specific time frame).

parameter	default
convert-to-static	**disable**
no-aging	**disable**
mac-move	**disable**
learn-as-static	**disable**
boot-up	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to clear the learning window time (no learning window time limit is applied to the port).
- The LPS source learning time window is started and/or reset each time the **port-security learning-window** command is issued or when the **port-security learning-window boot-up** option is enabled and the switch restarts.
- Setting the LPS learning window time to 0 (zero) configures an infinite source learning time period for all LPS ports. The learning of MAC addresses on LPS ports never times out.
- When the LPS learning window time is set to zero, all options except the **convert-to-static** option are still valid. For example, the **no-aging** option setting still applies.
- After the LPS learning window time expires, MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of bridged MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.
- Enabling the **no-aging** option triggers the following LPS learning window behavior:
  - All new bridged MAC addresses are learned as pseudo-static MAC addresses during the learning window time period. Pseudo-static addresses do not age out but are not saved to the switch configuration.
  - MAC movement is not allowed for pseudo-static MAC addresses unless the **mac-move** option is also enabled. The **mac-move** status (enabled or disabled) applies only to the **no-aging** option.

  - Enabling the **mac-move** option is not allowed unless the **no-aging** option is also enabled. When the **mac-move** option is enabled, disabling the **no-aging** option is *not* allowed.
  - When the learning window starts, any MAC addresses that were learned prior to the learning window time period are retained as dynamic addresses; they are not converted to pseudo-static MAC addresses.

- The **learn-as-static** and **no-aging** options are mutually exclusive; if both are enabled, then the **learn-as-static** option takes precedence.
- If the **convert-to-static** option is enabled, then all dynamic bridged and pseudo-static MAC addresses are converted to static MAC addresses when the learning window closes. Static MAC addresses do not age out and are saved to the switch configuration.

Note. When UNP is enabled on any one LPS port, the **convert-to-static**, **no-aging**, and **boot-up** parameter options are not supported on *all* LPS-enabled ports. This is because the learning window configuration is global and applies to all LPS ports.

Examples

```
-> port-security learning-window 25
-> port-security learning-window 2 convert-to-static enable
-> port-security learning-window 60 no-aging enable mac-move enable
-> port-security learning-window 0 learn-as-static enable
-> port-security learning-window 500 boot-up disable
-> port-security learning-window 2 convert-to-static enable no-aging enable
-> port-security learning-window 2 no-aging enable convert-to-static enable boot-up
enable learn-as-static enable mac-move enable
-> no port-security learning-window
```

Release History

Release 7.1.1; command introduced.
Release 7.2.1.R02; **no-aging** and **boot-up** parameters added.
Release 8.2.1; **learn-as-static** and **mac-move** parameters added.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security port max-filtering	Configures the maximum number of MAC addresses that can be filtered on the LPS port.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.
show port-security learning-window	Displays the source learning window configuration.

MIB Objects

```
learnedPortSecurityGlobalGroup
   lpsLearningWindowTime
   lpsLearningWindowTimeWithStaticConversion
   lpsLearningWindowNoAging
   lpsLearningWindowBootupStatus
   lpsLearningWindowLearnAsStatic,
   lpsLearningWindowPseudoMacMove
```

port-security convert-to-static

Converts all MAC addresses dynamically learned on the LPS port(s) to static MAC addresses. This command does not apply to MAC addresses that are filtered.

port-security {port *chassis/slot/port***[-***port2***]** | **chassis} convert-to-static**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
chassis	Specifies all the LPS ports on the chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Converting dynamic MAC addresses to static MAC addresses is not supported on Universal Network Profile (UNP) ports.
- You can stop the aging out of dynamic MAC addresses on the LPS port(s) by converting them to static MAC addresses.
- The number of converted static MAC addresses cannot exceed the maximum number of MAC addresses allowed on the port(s).

Note. The **port-security convert-to-static** command is not supported on UNP ports.

Examples

```
-> port-security port 4/8 convert-to-static
-> port-security chassis convert-to-static
```

Release History

Release 7.2.1.R02; command was introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

MIB Objects

```
learnedPortSecurityGlobalGroup
   lpsConvertToStatic
```

port-security mac

Configures a static MAC address on the specified LPS port. This command also enables LPS on the specified port, if LPS is not already active on the port.

port-security port *chassis/slot/port***[**-*port2***] mac** *mac_address* **[vlan** *vlan_id***]**

no port-security port *chassis/slot/port***[**-*port2***] mac [all |** *mac_address***] [vlan** *vlan_id***]**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
mac_address	MAC address to configure as a static MAC address on the specified LPS port (for example, 00:20:95:00:10:2A).
vlan	The VLAN ID to associate with the specified LPS port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to remove a specific static MAC address or all of the static MAC addresses configured on the specified LPS port. Note that even when all statically configured MAC addresses are removed, LPS remains active on the port.
- A VLAN-port association (VPS) must exist between the specified VLAN and the LPS port. If no VLAN ID is specified with this command, the default VLAN for the LPS port is used.
- The following conditions will display an error or warning message:
  - A VLAN ID is specified that is not associated with the LPS port:
  - An attempt is made to configure a MAC address more than once on the same LPS port with the same VLAN association.
  - A duplicate MAC address is configured on different LPS ports.
- Configuring a multicast MAC address, an all zero MAC address, or a broadcast MAC address is not allowed with this command.
- Use this command instead of the **mac-learning static mac-address** command to create a static MAC address on an LPS port.

Examples

```
-> port-security port 1/1/20 mac 00:20:95:00:fa:5c
-> port-security port 1/1/1-15 mac 00:da:95:00:00:10
-> no port-security port 1/1/20 mac 00:20:95:00:fa:5c
```

```
-> no port-security port 1/1/1-15 mac 00:da:95:00:00:10

-> port-security port 1/1/20 mac 00:2a:95:11:22:10 vlan 200
ERROR: Vlan 200 is not valid on this port

-> port-security port 1/1/20 mac 00:2a:95:11:22:10 vlan 200
-> port-security port 1/1/20 mac 00:2a:95:11:22:10 vlan 200
ERROR: Mac 00:2a:95:11:22:10 ALREADY exists on Vlan 200 for port 1/1/20

-> port-security port 1/1/20 mac 00:2a:95:11:22:10 vlan 200
-> port-security port 1/1/21 mac 00:2a:95:11:22:10 vlan 200
WARNING: LPS Static MAC 00:2a:95:11:22:10 already exists on vlan 200 on a different
port
```

Release History

Release 8.4.1; command introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security learning-window	Configures the amount of time in minutes to allow source learning on all LPS ports.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security port max-filtering	Configures the maximum number of MAC addresses that can be filtered on the LPS port.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.
show port-security	Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

```
learnedPortSecurityAgL2MacAddressTable
   lpsAgL2MacAddress
   lpsAgL2VlanId
   lpsAgL2MacAddressRowStatus
```

port-security maximum

Specifies the maximum number of bridged MAC addresses that an LPS port(s) is allowed to learn.

port-security port *chassis/slot/port***[**-*port2***]** **maximum** *number*

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
number	The number of source MAC addresses that are allowed on this port. The valid range is 1–1000.

Defaults

By default, the number of MAC addresses allowed is set to 1.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Any additional source MAC addresses received that exceed the maximum number of bridged addresses allowed are filtered on the port, regardless of the LPS learning window time limit. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.
- Note that source learning of configured authorized MAC addresses is still allowed after the LPS time limit has expired; however, all learning is stopped if the number of MAC addresses learned meets or exceeds the maximum number of addresses allowed, even if the LPS time limit has not expired.

Examples

```
-> port-security port 2/14 maximum 25
-> port-security port 4/10-15 maximum 100
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security learning-window	Configures the amount of time in minutes to allow source learning on all LPS ports.
port-security learn-trap-threshold	Configures the number of bridged MAC addresses to learn before sending a SNMP trap.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

```
learnedPortSecurityTable
   lpsMaxMacNum
```

port-security learn-trap-threshold

Configures the number of bridged MAC addresses to learn before sending a SNMP trap.

port-security port *chassis/slot/port***[**-*port2***] learn-trap-threshold** *number*

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
number	The number of bridged MAC addresses to learn before sending a trap. The valid range is 0–1000.

Defaults

By default, the number of bridged MAC addresses to learn before sending a trap is set to the same value as the maximum number of bridged MAC addresses allowed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the number of bridged MAC addresses learned on the port matches the specified threshold amount, a trap is sent for every bridged MAC address learned thereafter.
- Sending a trap when this threshold is reached provides notification of newly learned bridged MAC addresses. Trap contents includes identifying information about the MAC, such as the address itself, the corresponding IP address, switch identification, and the slot and port number on which the MAC was learned.
- If this threshold value is set to zero, a trap is sent for every MAC address learned on the LPS port.

Examples

```
-> port-security port 1/10 learn-trap-threshold 6
-> port-security port 1/10-13 learn-trap-threshold 18
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-security maximum	Configures the maximum number of source MAC addresses that an LPS port is allowed to learn.
show port-security	Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

```
learnedPortSecurityTable
   lpsLearnTrapThreshold
```

port-security port max-filtering

Configures the maximum number of MAC addresses that can be filtered on the LPS port(s).

port-security port *chassis/slot/port***[**-*port2***]** **max-filtering** *number*

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
number	The maximum number of filtered MAC addresses that are allowed on this port. The valid range is 0–100.

Defaults

By default, the maximum number of MAC addresses that can be filtered on an LPS port is 5.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the number of filtered MAC addresses learned on the port reaches the maximum, the violation mode (restrict, discard, or shutdown) configured for the port is applied.
- Any additional source MAC addresses received that exceed the maximum number of bridged addresses allowed are filtered on the port, regardless of the LPS learning window time limit. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.
- Even after the LPS learning window time expires, MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.

Examples

```
-> port-security port 1/10 max-filtering 6
-> port-security port 1/10-13 max-filtering 18
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security learning-window	Configures the amount of time in minutes to allow source learning on all LPS ports.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.
show port-security	Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

```
learnedPortSecurityTable
   lpsMaxFilteredMacNum
```

port-security mac-range

Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port. This command also enables LPS on the specified port, if LPS is not already active on the port.

port-security port *chassis/slot/port***[**-*port2***] mac-range [low** *mac_address* | **high** *mac_address***]**

no port-security port *chassis/slot/port***[**-*port2***] mac-range [low** *mac_address***]**

Syntax Definitions

*chassis/slot/port***[**-*port2***]**	The chassis, slot and port number (1/1/1). Use a hyphen to specify a range of ports (1/1/1-8). On the OmniSwitch 6900 only, configuring multiple MAC address ranges for the same port is supported.
low *mac_address*	MAC address that defines the low end of a range of MACs (for example, 00:20:95:00:10:2A).
high *mac_address*	MAC address that defines the high end of a range of MACs (for example, 00:20:95:00:10:2F).

Defaults

parameter	default
high *mac_address*	ff:ff:ff:ff:ff:ff
low *mac_address*	00:00:00:00:00:00

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- By default, each LPS port is set to a range of 00:00:00:00:00:00–ff:ff:ff:ff:ff:ff, which includes all MAC addresses.
- Source MAC addresses received on an LPS port that fall within the authorized range are allowed on the port. An additional entry is made in the LPS table for each of these learned addresses.
- Any additional source MAC addresses received that do not match the configured authorized addresses are not allowed (filtered) on the port, regardless of the LPS learning window time limit or the maximum number of bridged addresses allowed. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.
- Configuring more than one MAC address range per port is supported. When attempting to configure multiple MAC address ranges on the same port, consider the following:
  - A maximum of eight multiple MAC address ranges can be configured per port.
  - On a newly configured LPS port, the first user configured MAC range would overwrite the default MAC range.
  - A MAC range cannot overlap with another MAC range configured for the port.
  - Modifying a MAC range is allowed only if the lower MAC address is not changed and the defined new range does not overlap with the existing range. To modify the lower MAC address, the existing

range must be deleted before adding the new range.

- When modifying a MAC range, the new range must match or accommodate any existing static MACs on the port, else an error will be thrown indicating some static MACs exist on the port that fall outside the new/resultant MAC range being configured. (Note: It is required to flush such static MACs on the port, if user needs to configure the new MAC range, which was not accommodating the static MACs).
- When the MAC range size is increased, all the dynamic filtering MACs on the port would be flushed.
- When the MAC range size is reduced, any existing dynamic forwarding MACs learned on the port would be flushed if they fall outside any MAC ranges configured on the port at that point of time.
- All the dynamic filtering MACs learned on the port would be flushed.

- Use the **no** form of this command to delete the configured MAC range.
- The default MAC range is automatically applied when all the configured MAC ranges for the port are deleted.
- The default MAC range on the port cannot be deleted.

Examples

```
-> port-security port 1/5/11-15 mac-range low 00:da:95:00:00:10 high
00:da:95:00:00:1f
-> port-security port 1/1/5 mac-range low 00:01:01:22:22:56 high 00:01:01:22:22:67
-> port-security port 1/1/5 mac-range low 00:01:01:22:33:56 high 00:01:01:22:33:67
-> port-security port 1/1/5 mac-range low 00:01:01:22:44:56 high 00:01:01:22:44:67
-> port-security port 1/1/5 mac-range low 00:01:22:22:11:56 high 00:01:22:22:11:67
-> port-security port 1/1/5 mac-range low 00:01:22:22:22:56 high 00:01:22:22:22:67
-> port-security port 1/1/5 mac-range low 00:01:22:22:33:56 high 00:01:22:22:33:67
-> port-security port 1/1/5 mac-range low 00:01:22:22:44:56 high 00:01:22:22:44:67
-> port-security port 1/1/5 mac-range low 00:01:22:22:55:56 high 00:01:22:22:55:67
-> no port-security port 1/1/5 mac-range low 00:01:01:22:33:56
```

Release History

Release 7.1.1; command introduced.
Release 8.5R3; ability to configure multiple MAC ranges per port added.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security learning-window	Configures the amount of time in minutes to allow source learning on all LPS ports.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security port max-filtering	Configures the maximum number of MAC addresses that can be filtered on the LPS port.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.
show port-security	Displays the LPS configuration and table entries.
show port-security mac-range	Displays the MAC ranges configured on the LPS ports.

MIB Objects

```
learnedPortSecurityTable
   lpsLoMacRange
   lpsHiMacRange
   lpsRowStatus
learnedPortSecurityL2MacRangeTable
   lpsL2LowMacAddress
   lpsL2HighMacAddress
```

port-security port violation

Selects the method for handling traffic that does not comply with LPS restrictions for the specified port(s).

port-security port *chassis/slot/port***[**-*port2***] violation {shutdown | restrict | discard}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
shutdown	The port is administratively disabled when the port receives unauthorized traffic. No further traffic is allowed on the port.
restrict	Filters (blocks) unauthorized traffic but allows traffic that complies with LPS restrictions to forward on the port. The port remains administratively enabled.
discard	Disables learning on the port when unauthorized traffic is received or the configured maximum number of MAC addresses is reached. The port remains administratively enabled.

Defaults

By default, the security violation mode is set to **restrict** when LPS is enabled on the port.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When a traffic violation occurs on an LPS port, a notice is sent to the switch log.
- If the violation mode is set to **restrict**, unauthorized source MAC addresses are not learned in the LPS table, but they are recorded in the source learning MAC address table with a filtered operational status. This allows the user to view MAC addresses attempting unauthorized access to the LPS port.

Examples

```
-> port-security port 2/14 violation restrict
-> port-security port 4/10-15 violation shutdown
-> port-security port 1/37 violation discard
```

Release History

Release 7.1.1; command introduced.
Release 7.2.1.R02; **discard** parameter added.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
interfaces fec	Clears all port violations; allows the port to resume normal operation without a manual reset of the port or module.
show port-security	Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

```
learnedPortSecurityTable
   lpsViolationOption
```

show port-security

Displays the Learned Port Security (LPS) configuration and table entries.

show port-security {port [*chassis/slot/port***[-***port2***] | slot** *chassis/slot***]}**

Syntax Definitions

chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot	Enter the slot number for a module to specify that the command should include all ports on that module (for example, 6 specifies all ports on the module found in slot 6 of the switch chassis).

Defaults

By default, all ports with an LPS configuration are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Displays ports that have an LPS configuration, even if LPS is disabled on the port.
- Use the **port** parameter with this command to display the LPS configuration for a specific port or a range of ports.
- Use the **slot** parameter with this command to display the LPS configuration for all the ports on a specific slot.
- In addition, MAC addresses learned on the LPS enabled port that are within the specified MAC address range appear as a separate entries in the LPS table as dynamic MAC type addresses.
- The MAC Type field is blank if an authorized MAC address range is configured for the LPS port.

Examples

```
-> show port-security port 1/1/20
Legend: Mac Address: * = address not valid,

        Mac Address: & = duplicate static address,

Port:  1/1/20
 Admin-State      :               ENABLED,
 Operation Mode   :               ENABLED,
 Max MAC bridged  :                     3,
 Trap Threshold   :                     1,
 Violation        :              RESTRICT
 Max MAC filtered :                     5,
 Violating MAC    :                  NULL
```

```
           MAC              VLAN       MAC TYPE          OPERATION
------------------------+--------+-----------------+-----------------
 00:11:22:22:22:21           1       STATIC           bridging
 00:11:22:22:22:22           1       STATIC           bridging
 00:11:22:22:22:23           1       PSEUDO-STATIC    bridging
```

output definitions

Port	The module slot number and the physical port number on that module.
Admin-State	The LPS administrative state for the port (**Enabled**, **Disabled**, or **Locked**). Configured through the **port-security** command.
Operation Mode	The LPS operational mode for the port (**Enabled**, **Disabled**, **Restricted**, **Shutdown**, **Discard**, **Locked**, or **Filtered-only**).
Max MAC bridged	The maximum number of bridged MAC addresses that are allowed on this port. Configured through the **port-security maximum** command.
Trap Threshold	The number of bridged MACs to learn before sending a trap. After this number is reached, a trap is sent out for every MAC learned thereafter. If **disabled** is displayed in this field, the trap threshold is not in force. Configured through the **port-security learn-trap-threshold** command.
Violation	The security violation mode for the port (**restrict**, **shutdown**, or **discard**). Configured through the **port-security port violation** command.
Max MAC filtered	The maximum number of filtered MAC addresses that the LPS port can learn. Configured through the **port-security port max-filtering** command.
Violating MAC	The MAC Address that caused the violation on this port.
MAC	The MAC address learned dynamically or configured statically on the LPS port. Static MAC addresses configured through the **port-security mac** command.
VLAN	The VLAN to which the LPS port belongs.
MAC TYPE	Indicates if the MAC address was dynamically learned or statically configured as an authorized MAC address for the port.
OPERATION	The operational status of the MAC address (**bridging** or **filtering**).

Release History

Release 7.1.1; command introduced.
Release 7.2.1.R02: **Admin-State** and **Violating MAC** fields added.
Release 8.4.1; **MAC Address: * = address not valid** and **MAC Address: & = duplicate static address** legend added.

Related Commands

show port-security learning-window	Displays the amount of time during which source learning can occur on all LPS ports.

MIB Objects

```
learnedPortSecurityTable
   lpsAdminStatus
   lpsOperStatus
   lpsMaxMacNum
   lpsLearnTrapThreshold
   lpsViolationOption
   lpsMaxFilteredMacNum
   lpsLoMacRange
   lpsHiMacRange
   lpsViolatingMac
   lpsRelease
learnedPortSecurityAgL2MacAddressTable
   lpsAgL2MacAddress
   lpsAgL2VlanId
   lpsAgL2MacAddressLearnType
```

show port-security mac-range

Displays the MAC range configured on the Learned Port Security (LPS) ports.

show port-security [port *chassis/slot/port***[**-*port2***]] mac-range**

Syntax Definitions

*chassis/slot/port***[**-*port2***]**	The chassis, slot and port number (1/1/1). Use a hyphen to specify a range of ports (1/1/1-8).

Defaults

By default, all the LPS ports configured with MAC range are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Specify the chassis, slot, and port to view the MAC range configured for the specific port.

Examples

```
-> show port-security port 1/1/4 mac-range
Port:  1/1/4:
      Low MAC Range              High MAC Range
-------------------------+-------------------------
00:00:00:00:00:00             00:00:00:00:00:10
00:00:00:44:00:01             00:00:00:66:ff:ff

-> show port-security mac-range
Port:  1/1/2:
      Low MAC Range              High MAC Range
-------------------------+-------------------------
00:00:00:00:00:01             00:00:00:00:00:20
00:00:00:00:55:01             00:00:00:00:55:ff
00:00:00:66:00:01             00:00:00:99:ff:ff

Port:  1/1/4:
      Low MAC Range              High MAC Range
-------------------------+-------------------------
00:00:00:00:00:00             00:00:00:00:00:10
00:00:00:44:00:01             00:00:00:66:ff:ff
```

output definitions

Port	The chassis slot number and the physical port number on that chassis.
Low MAC Range	MAC address that defines the lower end of a MAC address range. Configured through the **port-security mac-range** command.
High MAC Range	MAC address that defines the higher end of a MAC address range. Configured through the **port-security mac-range** command.

Release History

Release 8.5R3; command introduced.

Related Commands

port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.

MIB Objects

```
learnedPortSecurityL2MacRangeTable
   lpsL2LowMacAddress
   lpsL2HighMacAddress
```

show port-security brief

Displays the LPS port configuration for all the LPS ports.

show port-security brief

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The LPS port parameter values are displayed even if the LPS is disabled on the port.
- The operation mode displayed for the LPS port is based on a combination of the existing administrative status and the operational status of the port, the result of which is one of the following values:
  - Enabled
  - Restricted (only when the administrative status is enabled)
  - Shutdown (only when the administrative status is enabled)
  - Discard (only when the administrative status is enabled)
  - Disabled
  - Locked
  - Filtered_only

Examples

```
-> show port-security brief
Slot/                  Max      Max      Nb Macs  Nb Macs    Nb Macs    Nb Macs
Port  Operation Mode   Bridge   Filter   Dyn Br   Dyn Fltr   Static Br  Static Fltr
----+----------------+--------+--------+---------+---------+-----------+-----------
1/1   ENABLED          5       100        5          10         0          0
1/2   ENABLED          5       100        0          10         5          0
1/3   RESTRICTED       5       100        5          100        0          0
1/4   SHUTDOWN         5       100        -          -          -          0
1/5   DISABLED         5       100        -          -          -          0
1/6   LOCKED           5       100        -          -          3          0
```

output definitions

Slot/Port	The slot number for the module and the physical port number on that module (e.g., 1/2 specifies port 2 on slot 1).
Operation Mode	Displays the status of the LPS port.

output definitions

Max Bridge	The maximum number of bridged MAC addresses that are allowed on the LPS port. Configured through the **port-security maximum** command.
Max Filter	The maximum number of filtered MAC addresses that the LPS port can learn. Configured through the **port-security port max-filtering** command.
Nb Macs Dyn Br	Total number of bridged MAC addresses learned on the LPS port.
Nb Macs Dyn Fltr	Total number of filtered MAC addresses learned on the LPS port.
Nb Macs Static Br	Total number of bridged static MAC addresses (configured static and MAC addresses learned as pseudo-static) on the LPS port.
Nb Macs Static Fltr	Total number of filtered static MAC addresses configured on the LPS port.

Release History

Release 7.2.1.R02; command was introduced.

Related Commands

show port-security	Displays the LPS configuration and table entries for individual LPS ports.

MIB Objects

```
learnedPortSecurityTable
   lpsMaxMacNum
   lpsMaxFilteredMacNum
   lpsMaxStaticMacNum
   lpsOperStatus
   lpsAdminStatus
```

show port-security learning-window

Displays the source learning window configuration.

show port-security learning-window

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The source learning time limit is a switch-wide parameter that applies to all ports that have LPS enabled.
- If the learning window time is not set, then no source learning time limit is applied to LPS ports.
- Even after the LPS learning window time expires, dynamic MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of bridged MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.

Examples

```
-> show port-security learning-window
Learning-Window             =  2 min,
Convert-to-static           =  DISABLE,
No Aging                    =  DISABLE,
Boot Up                     =  ENABLE,
Remaining Learning Window   =  120 sec
Learn As Static             =  ENABLE,
Mac Move                    =  DISABLE,
```

output definitions

Learning-Window	The configured amount of time during which the LPS port can learn new MAC addresses. This value of this field is set to **INFINITY** when the learning time window is set to zero (no source learning time restriction on LPS ports).
Convert-to-static	Indicates whether or not dynamic bridged or pseudo-static MACs are converted to static MACs (**ENABLED** or **DISABLED**). This option is always disabled when the LPS learning window is set to infinity (zero).

output definitions

No Aging	Indicates whether or not bridged MAC addresses are learned as pseudo-static MAC addresses, which do not age out during the LPS learning window time period (**DISABLED** or **ENABLED**).
Boot Up	Indicates whether or not the LPS learning window automatically starts when the switch boots up (**enabled** or **disabled**).
Learn As Static	Indicates whether or not dynamic MAC addresses are automatically learned as static MAC addresses during the LPS learning window time period. The **Learn As Static** and **No Aging** learning window options are mutually exclusive.
Mac Move	Indicates whether or not pseudo-static MAC addresses are allowed to move to a different port in the same VLAN during the LPS learning window time period. The **Mac Move** learning window option applies only when the **No Aging** option is enabled.
Remaining Learning Window	The remaining amount of time during which the LPS port can learn MAC addresses. If the learning time window is set to **INFINITY** (zero), this field does not display in the show command output.

Release History

Release 7.1.1; command introduced.
Release 7.2.1.R02; **LPS Shutdown Config** field changed to **Learning-Window**, **No Aging** and **Boot Up** fields added.
Release 8.2.1; **Learn As Static** and **Mac Move** fields added.

Related Commands

port-security learning-window	Configures the learning window parameters that are applied to all LPS ports.
show port-security	Displays the LPS configuration and table entries for individual LPS ports.

MIB Objects

```
learnedPortSecurityGlobalGroup
   lpsLearningWindowTime
   lpsLearningWindowTimeWithStaticConversion
   lpsLearningWindowNoAging
   lpsLearningWindowBootupStatus
   lpsLearningWindowLearnAsStatic,
   lpsLearningWindowPseudoMacMove
   lpsLearningWindowTimeRemaining
```

47 Port Mirroring and Monitoring Commands

The Port Mirroring and Port Monitoring features are primarily used as diagnostic tools.

The Port Mirroring feature allows you to have all the inbound and outbound traffic of an Ethernet port sent to another port on the switch. When you enable port mirroring, the active, or "mirrored," port transmits and receives network traffic normally and the "mirroring" port receives a copy of all transmit and receive traffic to the active port. You can connect an RMON probe or network analysis device to the mirroring port to see an exact duplication of traffic on the mirrored port without disrupting network traffic to and from the mirrored port.

The Port Monitoring feature allows you to capture and examine the data traffic to and from a monitored Ethernet port.

MIB information for the Port Mirroring commands is as follows:

Filename: ALCATEL-IND1-PORT-MIRRORING-MONITORING-MIB.mib
Module: alcatelIND1PortMirrorMonitoringMIB

The following table summarizes the available commands:

Port Mirroring Commands	**port-mirroring source destination** **port-mirroring** **show port-mirroring status**
Port Monitoring Commands	**port-monitoring source** **port-monitoring** **show port-monitoring status** **show port-monitoring file**

port-mirroring source destination

Defines the port to mirror and the port that is to receive data from the mirrored port. Also, enables or disables remote port mirroring.

port-mirroring *port_mirror_sessionid* **source {port** *chassis/slot/port***[-***port2***]} destination {port** *chassis/slot/port***[-***port2***]** | **linkagg** *linkagg***[-***linkagg2***]} [rpmir-vlan** *vlan_id***] [bidirectional |inport |outport] [unblocked-vlan** *vlan_id***] [tag-remove] [enable | disable]**

port-mirroring *port_mirror_sessionid* **no source {port** *chassis/slot/port***[-***port2***] [***chassis/slot/port***[-***port2***]...}**

port-mirroring *port_mirror_sessionid* **no destination {port** *chassis/slot/port***[-***port2***] [***chassis/slot/port***[-***port2***]...]** | **linkagg** *linkagg***[-***linkagg2***] [***linkagg***[-***linkagg2***]...}**

Syntax Definitions

port_mirror_sessionid	Mirroring session identifier.
source	Specifies source port, or range of ports desired to be mirrored.
destination	Specifies the destination port or linkagg that receives all the mirrored packets.
chassis	The chassis identifier.
*slot/port***[-***port2***]**	The slot and port number. Use a hyphen to specify a range of ports.
linkagg[-*linkagg2I*]	The destination link aggregate. Use a hyphen to specify a range. *This parameter is supported only on the OmniSwitch 6900, OmniSwitch 6860, and OmniSwitch 9900.*
rpmir-vlan *vlan_id*	Specifies a reserved VLAN to carry the mirroring traffic. Use this parameter to configure remote port mirroring. See "Usage Guidelines - Remote Port Mirroring" below for more information.
bidirectional	Specifies bidirectional port mirroring.
inport	Specifies incoming unidirectional port mirroring.
outport	Specifies outgoing unidirectional port mirroring.
unblocked-vlan *vlan_id*	Specifies the VLAN that is to be protected from Spanning Tree changes when port mirroring is active. Ports in this VLAN remain unblocked.
tag-remove	Removes the VLAN tag on mirrored traffic that egresses out of the destination mirroring ports. *This parameter is supported only on the OmniSwitch 9900.*
enable	Enables port mirroring status.
disable	Disables port mirroring status.

Defaults

parameter	default
bidirectional | inport | outport	**bidirectional**
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Port mirroring cannot be configured on an AppMon enabled port.
- You can configure a port mirroring and a port monitoring session on the same network interface module.
- A mirroring port can not be assigned to a tagged VLAN port.
- When a port is configured as a mirroring port, it does not belong to any VLAN. Inbound traffic to the mirroring port is dropped since it does not belong to any VLAN.
- To mirror traffic from SAP port to destination port, explicitly create a VLAN same as the SAP VLAN.
- Spanning tree is disabled by default on a mirroring port.
- Port mirroring is not supported on logical link aggregate ports. However, it is supported on individual ports that are members of a link aggregate.
- Port mirroring destination port can be a link aggregate. This functionality is supported on OmniSwitch 6900 and OmniSwitch 6860 platforms only.
- Use the **port mirroring source destination** command to define the mirrored port and enable port mirroring status. Use the **port mirroring** command to enable the port mirroring session.
- Specify the *vlan_id* number of the mirroring port that is to remain **unblocked** when the command is executed. The **unblocked** VLAN becomes the default VLAN for the mirroring port. This VLAN handles the inbound traffic for the mirroring port. Spanning Tree remains disabled on the unblocked VLAN.
- A maximum of 128 source mirroring ports can be configured. In case of mirroring to LACP Link Aggregate, only the first 8 aggregable ports will be used for mirroring.
- Unblocked VLAN and RPMIR configuration cannot co-exist in the same port mirroring session.
- A port/link aggregate which is to be configured as a mirroring destination should have no prior configuration on it, for example, a MVRP enabled port/link aggregate cannot be configured as a mirroring destination. The only exception to this rule is that a port can be a untagged or a tagged member of a standard VLAN.
- Any protocol/feature configurations on existing mirroring destinations would fail. All such configuration attempts would result in an error. The only exception to this is that if a mirroring destination is part of a mirroring session which has remote port mirroring VLAN configured (RPMIR VLAN) then such a destination can be made a tagged and/or untagged member of standard VLAN(s).
- Supports single destination mirroring port per session and seven port mirroring sessions in a system on OmniSwitch 6560 and OmniSwitch 6465 platforms.
- Supports multiple destination mirroring port and link aggregates per session and seven port mirroring sessions, and 128 destination mirroring ports or link aggregates in a system. This functionality is supported on OmniSwitch 9900.

- Supports policy based multiple destination mirroring on a single port mirroring session. This functionality is supported on OmniSwitch 9900.
  - To enable this functionality, configure port mirroring session with destination port and then apply policy based configuration on the port mirroring session.
  - Use the QoS mirror session attribute to support policy based multiple destination mirroring. QoS mirroring session attribute can be specified as a part of policy action in the command **policy action** command. Mirroring can be done on the ingress packets only. Only one session ID is supported for policy based mirroring, thus all the policies must specify the same session ID. For more information on policy based mirroring, see **QoS Commands** chapter.
- Use the **tag remove** option to remove the VLAN tag on mirrored traffic that egresses out of destination mirroring ports. For double tagged mirrored packet, this option removes the outer VLAN tag.
- RPMIR and **tag remove** configuration is mutually exclusive and hence cannot co-exist in the same port mirroring session.

Usage Guidelines - Remote Port Mirroring

- Use the **rpmir-vlan** parameter and VLAN ID with this command to configure remote port mirroring and to assign the VLAN ID for remote port mirroring. Note that remote port mirroring is *not* supported on the OmniSwitch 6900-C32, OmniSwitch 6900-V72, and OmniSwitch 9900.
- The VLAN ID assigned for remote port mirroring cannot be assigned to a general port mirroring port.
- There must not be any physical loop present in the remote port mirroring VLAN.
- Source learning must be disabled or overridden on the ports belonging to the remote port mirroring VLAN on intermediate and destination switches.
- The QoS redirect feature can be used to override source learning.
- The **mac-learning** command can also be used to disable learning on the RPMIR VLAN ID.
- VLAN 1 cannot be configured as the RPMIR VLAN.
- When mirroring configuration is removed from a mirroring destination, the port/link aggregate is made an untagged member of VLAN 1. The only exception to this is when the destination in a mirroring session with RPMIR configuration.

Examples

```
-> port-mirroring 6 source port 1/2/2 destination port 1/1/3
-> port-mirroring 6 destination port 1/1/3 rpmir-vlan 7
-> port-mirroring 6 no source port 1/2/2

-> port-mirroring 7 source port 1/2/3 destination linkagg 3 unblocked-vlan 750
-> port-mirroring 7 source port 1/2/3 outport

-> port-mirroring 7 source port 1/2/3 destination linkagg 3 tag-remove

-> port-mirroring 9 source port 1/1/23 destination port 1/1/24
-> port-mirroring 9 disable
```

Release History

Release 7.1.1; command introduced.
Release 8.4.1.R03; Mirroring to a link aggregate supported on OmniSwitch 6900 and OmniSwitch 6860.

Release 8.6.R1; **tag-remove** keyword added, policy based multiple destination mirroring supported on OmniSwitch 9900.

Related Commands

port-mirroring	Enables, disables, or deletes a port mirroring session.
show port-mirroring status	Displays the status of mirrored ports. This value may be enabled or disabled.

MIB Objects

```
mirrorTable
   mirrorMirroringIfindex
   mirrorDirection
   mirrorStatus
   mirrorUnblockedVLAN
   mirrorRowStatus
   mirrorDirection
   mirrorSessOperStatus
   mirrorTaggedVLAN
   mirrorDstTagRemove
```

port-mirroring

Enables, disables, or deletes a port mirroring session.

port-mirroring *port_mirror_sessionid* **{enable | disable}**

no port-mirroring *port_mirror_sessionid*

Syntax Definitions

port_mirror_sessionid	Mirroring session identifier.
enable	Enables port mirroring.
disable	Disables port mirroring.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete a port mirroring session.
- Use the **port-mirroring source destination** command to specify the mirrored ports and destination port. before using this command to enable or disable port mirroring activity for the particular port mirroring session.

Examples

```
-> port-mirroring 6 enable
-> port-mirroring 6 disable
-> no port-mirroring 6
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-mirroring source destination	Defines a port to mirror and the port that is to receive data from the mirrored port, and enables or disables port mirroring status.
show port-mirroring status	Displays the status of mirrored ports. This value may be enabled or disabled.

MIB Objects

```
mirrorTable
   mirrorMirroringIfindex
   mirrorTaggedVLAN
   mirrorStatus
```

port-monitoring source

Configures a port monitoring session.

port-monitoring *port_monitor_sessionid* **source port** *chassis/slot/port***[**-*port2***] [file** *filename* **[size** *filesize***] | no file | overwrite {on | off}] [inport | outport | bidirectional] [timeout** *seconds***] [enable | disable] [capture-type {full | brief}]**

port-monitoring *port_monitor_sessionid* **no source port** *chassis/slot/port***[**-*port2***]**

Syntax Definitions

port_monitor_sessionid	Monitoring session identifier.
chassis	The chassis identifier.
*slot/port***[**-*port2***]**	The slot and port number. Use a hyphen to specify a range of ports.
filename	Specifies a file name and pathname for capturing information related to the monitoring session (for example, **/flash/port2.enc**).
filesize	Specifies the size of the file in 64K byte increments. For example, a value of 3 would specify a size of (3 x 64K) bytes.
no file	*This option is not supported at this time.*
on	Specifies that capturing of data packets into the port monitoring file continues and old information is overwritten if the total data exceeds the specified file size.
off	Specifies that capturing of data packets into the port monitoring file is stopped when the maximum file size is reached.
inport	Specifies incoming unidirectional port monitoring.
outport	Specifies outgoing unidirectional port monitoring.
seconds	Specifies the number of seconds after which the session is disabled.
enable	Enables the port monitoring status.
disable	Disables the port monitoring status.
full	Captures port monitoring information in detail.
brief	Captures only the concise port monitoring data transmitted.

Defaults

parameter	default
filesize	1
on | off	**on**
bidirectional | inport | outport	**bidirectional**
seconds	0
enable | disable	**disable**
capture-type	**brief**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Port monitoring cannot be configured on an AppMon enabled port.
- You can configure a port mirroring and a port monitoring session on the same NI.
- If the port monitoring capture-type is set to **brief**, the first 64 bytes of the traffic is captured. If the port-monitoring capture-type is set to **full**, the entire packet is captured.
- By default, a file called **pmonitor.enc** is created in the **/flash** directory when you configure and enable a port monitoring session. Use the **file** option to create a user-specified file.
- The **/flash** directory is the default and the only directory used to capture the port monitoring files.
- The format of the file created is compliant with the ENC file format (Network General Sniffer Network Analyzer Format).
- By default, the recent frames overwrite the older frames in a port monitoring file if the total data exceeds the specified file size. Use the **overwrite off** option to prevent this from occurring.

Examples

```
-> port-monitoring 6 source port 1/2/3
-> port-monitoring 6 source port 1/2/3 file /flash/user_port size 2 enable
-> port-monitoring 6 source port 1/2/3 file /flash/user_port capture-type full
-> port-monitoring 10 source port 1/4/22-30
-> port-monitoring 10 no source port 1/4/30
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-monitoring	Disables, pauses, resumes, or deletes a port monitoring session.
show port-monitoring status	Displays the port monitoring status.
show port-monitoring file	Displays the port monitoring data.

MIB Objects

```
monitorTable
   monitor
   monitorSessionNumber
   monitorIfindex
   monitorFileStatus
   monitorFileName
   monitorFileSize
   monitorScreenStatus
   monitorScreenLine
   monitorCaptureType
   monitorTrafficType
   monitorStatus
   monitorFileOverWrite
   monitorDirection
   monitorTimeout
```

port-monitoring

Disables, pauses, resume, or deletes an existing port monitoring session.

port-monitoring *port_monitor_sessionid* **{disable | pause | resume}**

no port-monitoring *port_monitor_sessionid*

Syntax Definitions

port_monitor_sessionid	Monitoring session identifier.
disable	Disables the port monitoring session.
pause	Pauses the port monitoring session.
resumes	Resumes the port monitoring session.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **no** form of this command to delete a port monitoring session.

Examples

```
-> port-monitoring 6 pause
-> port-monitoring 6 disable
-> port-monitoring 6 resume
-> no port-monitoring 6
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-monitoring	Configures a port monitoring session.
show port-monitoring status	Displays the port monitoring status.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorScreenStatus
```

show port-mirroring status

Displays the status of mirrored ports.

show port-mirroring status [*port_mirror_sessionid***]**

Syntax Definitions

port_mirror_sessionid	Mirroring session identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If a port mirroring session identifier is not specified with this command, then all port mirroring sessions are displayed.

Examples

```
-> show port-mirroring status
 Session    Mirror        Mirror      Unblocked   RPMIR     Config    Oper
           Destination    Direction     Vlan       Vlan     Status    Status
----------+-----------+----------------+--------+---------+-------+---------
     1.     1/1/11       bidirectional  NONE      NONE      Enable    on
----------+-----------+----------------+--------+---------+---------+---------
         Mirror
         Source
----------+-----------+--------------+----------+---------+----------+---------
     1.      1/1/2       bidirectional     -         -      Enable    On
     1.      1/1/3       bidirectional     -         -      Enable    On
     1.      1/1/4       bidirectional     -         -      Enable    On
     1.      1/1/5       bidirectional     -         -      Enable    On
```

output definitions

Session	The port mirroring session identifier.
Mirror Destination	The location of the mirrored port.
Mirror Direction	The direction of the mirroring or mirrored port, which can be **bidirectional** (the default), **inport**, or **outport**.
Unblocked VLAN	The mirroring VLAN ID number.
RPMIR VLAN	The reserved VLAN to carry the mirroring traffic.
Config Status	The configuration status of the session.
Oper Status	The current status of the mirroring or mirrored port.
Mirror Source	The location of the mirroring port.

Release History

Release 7.1.1; command introduced.

Related Commands

port-mirroring	Enables, disables, or deletes a port mirroring session.
port-mirroring source destination	Defines a port to mirror and a port that receives data from the mirrored port, and enables or disables port mirroring status.

MIB Objects

```
mirrorTable
   mirrorMirroringIfindex
   mirrorMirroredIfindex
   mirrorDirection
   mirrorStatus
   mirrorSessionNumber
   mirrorSessOperStatus
   mirrorSrcStatus
   mirrorSrcDirection
   mirrorSrcRowStatus
   mirrorSrcOperStatus
   mirrorUnblockedVLAN
```

show port-monitoring status

Displays port monitoring status.

show port-monitoring status [*port_monitor_sessionid***]**

Syntax Definitions

port_monitor_sessionid Monitoring session identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If a port monitoring session identifier is not specified with this command, then all port monitoring sessions are displayed.

Examples

```
-> show port-monitoring status

 Sess Mon. Mon. Over  Oper.  Admin  Capt.   Max.   File
      Src  Dir  write Stat   Stat   Type    Size   Name
-----+----+----+-----+------+------+-------+------+-------------------------
  1.  1/1/2   Out  OFF    OFF   OFF   Brief     64K  /flash/pm.enc
```

output definitions

Sess	**Session** - The port monitoring session identifier.
Mon. Src	**Monitor Source** - The source ports that are monitored.
Mon Dir	**Monitor Direction** - The direction of the monitoring session, which can be **bidirectional** (the default), **inport**, or **outport**.
Overwrite	Whether files created by a port monitoring session can be overwritten. The default is ON.
Oper Stat	**Operating Status** - The current operating status of the port monitoring session (on/off).
Admin Stat	**Admin Status** - The current administrative status of the port monitoring session (on/off).
Capt Type	**Capture type**: **Brief** - captures only 64 bytes of data per traffic data packet. **Full** - captures the entire packet.
Max Size	**Maximum Size** - The maximum size of the port monitoring file.
File Name	The name of the port monitoring file.

Release History

Release 7.1.1; command introduced.

Related Commands

port-monitoring source	Configures a port monitoring session.
port-monitoring	Disables, pauses, resumes, or deletes a port monitoring session.
show port-monitoring file	Displays port monitoring data.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorIfindex
   monitorStatus
   monitorFileStatus
   monitorFileName
   monitorFileSize
   monitorScreenStatus
   monitorScreenLine
   monitorTrafficType
   monitorDirection
   monitorTimeout
   monitorCaptureType
   monitorFileOverWrite
   monitorDirection
```

show port-monitoring file

Displays port monitoring data.

show port-monitoring file *port_monitor_sessionid*

Syntax Definitions

port_monitor_sessionid	Monitoring session identifier.

Defaults

A single line from the captured packet is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Only a single line from the captured packet is displayed, even though the full packet is captured.To view the entire packet, download the file and view it using compatible network analyzer tool.

Examples

```
-> show port-monitoring file 1

Destination       | Source            |  Type  | Data
------------------------------------------------------------------------------
01:80:C2:00:00:00 | 00:20:DA:8F:92:C6 |  BPDU  | 00:26:42:42:03:00:00:00:00:00
00:20:DA:C7:2D:D6 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:FE:4A:40:00
00:20:DA:A3:89:F6 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:89:40:00
00:20:DA:BF:5B:76 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:85:40:00
00:20:DA:A3:89:F6 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:8A:40:00
00:20:DA:BF:5B:76 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:86:40:00
00:20:DA:A3:89:F6 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:8B:40:00
01:80:C2:00:00:00 | 00:20:DA:8F:92:C6 |  BPDU  | 00:26:42:42:03:00:00:00:00:00
00:20:DA:BF:5B:76 | 08:00:20:95:F3:89 |  UDP   | 08:00:45:00:00:6B:CF:87:40:00
```

output definitions

Destination	The destination MAC address of the packet.
Source	The source MAC address of the packet.
Type	The type of packet.
Data	The packet displayed in hexadecimal format.

Release History

Release 7.1.1; command introduced.

Related Commands

port-monitoring source	Configures a port monitoring session.
port-monitoring	Disables, pauses, resumes, or deletes a port monitoring session.
show port-monitoring status	Displays the port monitoring status.

MIB Objects

```
monitorTable
   monitorSessionNumber
   monitorIfindex
   monitorTrafficType
   monitorFileStatus
   monitorFileName
   monitorFileSize
   monitorScreenStatus
   monitorScreenLine
```

48 sFlow Commands

sFlow is a network monitoring technology that gives visibility in to the activity of the network, by providing network usage information. It provides the data required to effectively control and manage the network usage. sFlow is a sampling technology that meets the requirements for a network traffic monitoring solution.

sFlow provides a network-wide view of usage and active routes. It is used for measuring network traffic, collecting, storing, and analyzing the traffic data. As it is scalable, that doesn't add significant network load. sFlow is an industry standard with many vendors delivering products with this support. Some of the applications of the sFlow data include:

- Detecting, diagnosing, and fixing network problems
- Real-time congestion management
- Detecting unauthorized network activity
- Usage accounting and billing
- Understanding application mix
- Route profiling and peer optimization
- Capacity planning

sFlow is a sampling technology embedded within switches/routers. It provides the ability to monitor the traffic flows. It requires an sFlow agent software process running as part of the switch software and a sFlow collector which receives and analyses the monitored data. The sFlow collector makes use of SNMP to communicate with an sFlow agent in order to configure sFlow monitoring on the device (switch).

An sFlow agent running on the switch/router combines interface counters and traffic flow (packet) samples, preferably, on all the interfaces into sFlow datagrams that are sent across the network to an sFlow collector.

Packet sampling on the switch/router is typically performed by the switching/routing ASICs, providing wire-speed performance. In this case, an sFlow agent does very little processing, by packaging data into sFlow datagrams that are immediately sent on network. This minimizes the memory and CPU utilization by the sFlow agent.

MIB information for the sFlow commands is as follows:

Filename: ALCATEL-IND1-PORT-MIRRORING-MONITORING-MIB.mib
Module: alcatelIND1PortMirrorMonitoringMIB

Filename: SFLOW-MIB.MIB.mib
Module: sFlow

A summary of the available commands is listed here:

sflow agent
sflow receiver
sflow sampler
sflow poller
show sflow agent
show sflow receiver
show sflow sampler
show sflow poller

sflow agent

Configures a specific sFlow agent IP address.

sflow agent ip *ip_address*

no sflow agent ip *ip_address*

Syntax Definitions

ip_address	The sFlow agent IP address.

Defaults

parameter	default
ip-address	0.0.0.0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to delete the IP address.
- If no IP address is configured, 0.0.0.0 is used.
- If no IP address is configured but the Loopback0 address is configured, the Loopback0 address is used.

Examples

```
-> sflow agent ip 192.168.1.1
-> no sflow agent ip 192.168.1.1
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; command deprecated. Use **ip service source-ip.**

Related Commands

show sflow agent	Displays the agent table.

MIB Objects

```
mirmonSFlowObjects
   alasFlowAgentConfigType
   alasFlowAgentAddressType
   alasFlowAgentAddress
```

sflow receiver

Sets the destination hosts where the sFlow datagrams are sent out. If there are multiple destinations, then each destination has an instance of the receiver. All these receivers are attached to the sFlow manager instance and to an associated sampler/poller.

sflow receiver *receiver_index* **{name** *string* **| timeout {***seconds* **| forever} | address {***ip_address* **|** *ipv6_address* **|** *domain_name***} | udp-port** *port* **| packet-size** *size* **version** *num* **| release}**

Syntax Definitions

receiver_index	The receiver index number.
string	The name.
seconds | **forever**	Specifies the timeout value.
ip_address	Specifies the 32-bit IPv4 address.
ipv6_address	Specifies the 128-bit IPv6 address.
domain_name	Specifies a Fully Qualified Domain Name (FQDN). The domain name can be up to 255 characters in length.
port	Specifies the UDP (destination) port.
size	Specifies the maximum number of data bytes (size) that can be sent.
num	Specifies the version number.

Defaults

parameter	default
string	empty
seconds	0
ip_address	0.0.0.0(ipv4)
port	6343
size	1400
version num	5

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **release** parameter at the end of the command to delete a receiver.
- Use the *domain_name* option to specify an FQDN instead of an IPv4 or IPv6 address. The switch will then resolve the domain name to an IP address. Make sure the specified domain name maps to a valid and reachable address. If the address is not valid or cannot be reached, then flow and counter samples may not be sent out of the sFlow agent as expected.

- After the IPv4 or IPv6 address for the specified domain name is determined, a refresh is triggered every 30 seconds. If the mapping of the domain name to an IP address changes before the next refresh, both flow and counter samples are not sent to the new address until the next refresh occurs.

Examples

```
-> sflow receiver 1 name Golden Rcvr1 address 198.206.181.3
-> sflow receiver 1 name Golden Rcvr1 address upam.omnivista.com
-> sflow receiver 1 release
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R1; *domain_name* parameter option added.

Related Commands

show sflow receiver	Displays the receiver table.

MIB Objects

```
sFlowRcvrTable
   sFlowRcvrIndex
   sFlowRcvrOwner
   sFlowRcvrTimeout
   sFlowRcvrMaximumDatagramSize
   sFlowRcvrAddressType
   sFlowRcvrAddress
   sFlowRcvrPort
   sFlowRcvrDatagramVersion
```

sflow sampler

Gets the hardware sampled from Q-dispatcher and fills up the sampler part of the UDP datagram.

sflow sampler *num* **port** *chassis/slot/port***[-***port***] {receiver** *receiver_index* **| rate** *value* **| sample-hdr-size** *size***}**

no sflow sampler *num* **port [***chassis_id/***]***slot/port***[-***port***]**

Syntax Definitions

num	Specifies the instance ID.
chassis	The chassis identifier.
*slot/port***[-***port***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).
receiver_index	Specifies the receiver index.
value	Specifies the rate value for packet sampling.
size	Specifies the maximum number of bytes (size) that can be copied from a sampled packet.

Defaults

parameter	default
receiver_index	0
value	0
size	128

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to delete a sampler.
- A sampling rate of 1 counts all packets. A sampling rate of 0 disables sampling.

Examples

```
-> sflow sampler 1 port 1/2/1 receiver 1 rate 5 sample-hdr-size 64
-> no sflow sampler 1 port 1/2/1-5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show sflow sampler	Displays the sampler table.

MIB Objects

```
sFlowFsTable
   sFlowFsDataSource
   sFlowFsInstance
   sFlowFsReceiver
   sFlowFsPacketSamplingRate
   sFlowFsMaximumHeaderSize
```

sflow poller

Gets counter samples from ethernet driver and fills up the counter part of the UDP datagram.

sflow poller *num* **port** *chassis/slot/port***[**-*port***] {receiver** *receiver_index* **| interval** *value***}**

no sflow poller *num* **port [***chassis_id/***]***slot/port***[**-*port***]**

Syntax Definitions

num	Specifies the instance ID.
chassis	The chassis identifier.
*slot/port***[**-*port***]**	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).
receiver_index	Specifies the receiver index.
value	Specifies the maximum number of seconds between successive samples (interval value).

Defaults

parameter	default
receiver_index	0
value	0

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

Use the **no** form of this command to delete a poller.

Examples

```
-> sflow poller 1 port 1/1/1 receiver 2 interval 20
-> sflow poller 1 port 1/2/6-10 receiver 1 interval 30
-> no sflow poller 1 port 1/2/6-10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show sflow poller	Displays the poller table.

MIB Objects

```
sFlowCpTable
   sFlowCpDataSource
   sFlowCpInstance
   sFlowCpReceiver
   sFlowCpInterval
```

show sflow agent

Displays the sFlow agent table.

show sflow agent

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- It is necessary to execute the **ip interface** command to make a loopback0 IP address as the fixed primary address of the switch to avoid interface changes, which might need the collector software to be restarted for it to communicate using the new agent IP address. Normally, the primary IP address could change depending on the IP interface going up/down. Therefore, the sFlow agent always needs to send a fixed IP address in the datagram.
- The loopback address should be an IP interface configured on the switch.

Examples

```
-> ip interface loopback0 address 198.206.181.100
-> show sflow agent
Agent Version  = 1.3; Alcatel; 6.1.1
Agent IP       = 127.0.0.1
```

output definitions

Agent Version	Identifies the version which includes the MIB version, organization name, and the specific software build of the agent.
Agent address	IP address associated with the agent. Configured through the **sflow agent** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show sflow receiver	Displays the receiver table.

MIB Objects

```
sFlowAgent
   sFlowVersion
   sFlowAgentAddressType
   sFlowAgentAddress
```

show sflow receiver

Displays the sFlow receiver table.

show sflow receiver [*num***]**

Syntax Definitions

num	Specifies the receiver index.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show sflow receiver
Receiver 1
Name       = Golden
Address    = IP_V4  198.206.181.3
UDP Port   = 6343
Timeout    = 65535
Packet Size= 1400
DatagramVer= 5

-> show sflow receiver

 Receiver 1
 Name       = Golden
 Address    = Domain Name  upam.omnivista.com IP_V4  198.206.181.3
 UDP Port   = 6343
 Timeout    = 65535
 Packet Size= 1400
 DatagramVer= 5
```

output definitions

Name	Name of the entry to claim.
Address	IP address of the sFlow collector. If a receiver address was configured as a domain name, then both the domain name and IP address for that domain are displayed. If the domain name did not translate to a valid IP address, a hyphen is displayed instead of an address.
UDP Port	Destination port for sFlow datagrams.
Timeout	Time remaining before the sampler is released and stops sampling.

output definitions

Packet size	Maximum number of data bytes that can be sent in a single sample datagram.
Datagram ver	Version of sFlow datagrams that should be sent.

Release History

Release 7.1.1; command was introduced.

Related Commands

sflow receiver	Sets the destination hosts where the sFlow datagrams are sent out.

MIB Objects

```
sFlowRcvrTable
   sFlowRcvrIndex
```

show sflow sampler

Displays the sFlow sampler table.

show sflow sampler [*num***]**

Syntax Definitions

num	Specifies the instance ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

N/A.

Examples

```
-> show sflow sampler
Instance   Interface    Receiver  Sample-rate   Sample-hdr-size
-----------------------------------------------------------------
   1         2/1/1          1         2048             128
   1         2/1/2          1         2048             128
   1         2/1/3          1         2048             128
   1         2/1/4          1         2048             128
   1         2/1/5          1         2048             128
```

output definitions

Instance	Instance for the flow sampler.
Interface	Interface used for the flow sampler.
Receiver	Receiver associated with the flow sampler.
Sample-rate	Statistical sampling rate for packet sampling from the source.
Sample-hdr-size	Maximum number of bytes that should be copied from a sampled packet.

Release History

Release 7.1.1; command was introduced.

Related Commands

sflow sampler	Gets hardware sampled from Q-dispatcher.

MIB Objects

```
sFlowFsTable
   sFlowFsInstance
```

show sflow poller

Displays the sFlow poller table.

show sflow poller [*num***]**

Syntax Definitions

num	Specifies the instance ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show sflow poller
Instance   Interface    Receiver  Interval(Secs)
----------------------------------------
     1        2/1/6         1         30
     1        2/1/7         1         30
     1        2/1/8         1         30
     1        2/1/9         1         30
     1        2/1/10        1         30
```

output definitions

Instance	Instance for the counter poller.
Interface	Interface used for the counter poller.
Receiver	Receiver associated with the counter poller.
Interval	The maximum number of seconds between successive samples of the counters associated with the data source.

Release History

Release 7.1.1; command was introduced.

Related Commands

sflow poller	Gets counter samples.

MIB Objects

```
sFlowCpTable
   sFlowCpInstance
```

49 RMON Commands

Remote Network Monitoring (RMON) probes can be used to monitor, manage, and compile statistical data about network traffic from designated active ports in a LAN segment without negatively impacting network performance. This feature supports basic RMON 4 group implementation compliant with RFC 2819 (Remote Network Monitoring Management Information Base), but does not support RMON 10 group or RMON 2. This chapter includes descriptions of RMON commands used to enable or disable individual (or a group of a certain flavor type) RMON probes, show a list of (or individual) RMON probes and show a list of (or individual) RMON logged events.

MIB information for the RMON commands is as follows:

Filename: RMON-MIB.mib
Module: rmonMibModule

The following table summarizes the available commands:

rmon probes
show rmon probes
show rmon events

rmon probes

This command enables or disables types of RMON probes.

rmon probes {stats | history | alarm} [*entry_number***] {enable | disable}**

Syntax Definitions

stats	Ethernet Statistics Table probe entries.
history	History Control Table probe entries.
alarm	Alarm Table probe entries.
entry_number	The entry number in the list of probes *(optional)*.
enable	Enables the RMON probe.
disable	Disables the RMON probe.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Network activity on subnetworks attached to the RMON probe can be monitored by NMS applications.
- RMON will not monitor activities on the CMM onboard Ethernet Management port.

Examples

```
-> rmon probes stats 4012 enable
-> rmon probes history 10240 disable
-> rmon probes alarm 11235 enable
-> rmon probes stats enable
-> rmon probes history disable
-> rmon probes alarm enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show rmon probes	Displays a list of RMON probes or a single RMON probe.
show rmon events	Displays a list of RMON logged events or a single RMON event.

MIB Objects

```
ETHERSTATSTABLE
   etherStatsStatus
HISTORYCONTROLTABLE
   historyControlStatus
ALARMTABLE
   alarmStatus
```

show rmon probes

Displays a list of RMON probes or a single RMON probe.

show rmon probes [stats | history | alarm] [*entry_number***]**

Syntax Definitions

stats	Ethernet Statistics Table probe entries.
history	History Control Table probe entries.
alarm	Alarm Table probe entries.
entry_number	The entry number in the list of probes *(optional)*.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- To display a list of current probes, omit the *entry-number* from the command line.
- To display statistics for a particular probe, include the probe's *entry_number* in the command line.
- The **show rmon probes** command displays the following information: Entry number, Slot/Port, Flavor (whether the probe type is Ethernet, History or Alarm), Status (Active or Inactive), Duration (time since the last change in status, in hours/minutes) and System Resources (the amount of memory allocated to this probe).
- The **show rmon probes** *entry-number* command displays the following information: Probe's Owner (probe type and location), Slot/Port, Entry number, Flavor (whether the probe type is Ethernet, History or Alarm), Status (Active or Inactive), Time since the last change in status (hours/minutes), and System Resources (the amount of memory allocated to this probe). Displayed statistics may vary, depending on whether the probe type is Ethernet, History or Alarm.

Examples

```
-> show rmon probes stats

        Chassis/
Entry  Slot/Port  Flavor    Status      Duration     System Resources
-------+----------+---------+-----------+------------+----------------
   1026 1/1/26     Ethernet  Active      71:49:41     301 bytes
   1025 1/1/25     Ethernet  Active      71:49:20     301 bytes
   1001 1/1/1      Ethernet  Active      71:48:05     300 bytes
```

```
-> show rmon probes history

          Chassis/
   Entry  Slot/Port    Flavor    Status      Duration     System Resources
   -------+---------+---------+-----------+------------+---------------
      1     1/1/26     History   Active      71:50:08     5471 bytes
      2     1/1/25     History   Active      71:49:47     5471 bytes
      3     1/1/1      History   Active      71:48:32     5470 bytes
      4     1/1/22     History   Active      71:48:30     5471 bytes
      5     1/1/23     History   Active      71:48:30     5471 bytes

-> show rmon probes alarm

Entry    Slot/Port   Flavor     Status       Duration          System Resources
-------+-----------+-----------+----------+---------------+---------------------
11235    1/4/8       Alarm       Active      00:07:00          835 bytes


   -> show rmon probes 4005

   Probe's Owner: Switch Auto Probe on Chassis 1, Slot 4, Port 5, ifindex 4005
       Entry    4005
         Flavor = Ethernet, Status = Active,
         Time = 48 hrs 54 mins,
      System Resources (bytes) = 301

   -> show rmon probes history 30562

   Probe's Owner: Switch Auto Probe on Chassis 8, Slot 1, Port 29
     History Control Buckets Requested = 50,
     History Control Buckets Granted   = 50,
     History Control Interval          = 30 seconds,
     History Sample Index              = 287
       Entry       9
         Flavor = History, Status = Active,
         Time = 71 hrs 48 mins,
      System Resources (bytes) = 5471

-> show rmon probes alarm 11235

Probe’s Owner:
  Alarm Rising Threshold         = 5
  Alarm Falling Threshold        = 0
  Alarm Rising Event Index       = 26020
  Alarm Falling Event Index      = 0
  Alarm Interval                 = 10 seconds
  Alarm Sample Type              = delta value
  Alarm Startup Alarm            = rising alarm
  Alarm Variable = 1.3.6.1.2.1.16.1.1.1.5.4008
   Entry 11235
      Flavor = Alarm, Status = Active
      Time = 48 hrs 48 mins,
      System Resources (bytes) = 1677
```

output definitions

Probe's Owner	Description and interface (location) of the probe.
Slot/Port	The Slot/Port number (interface) that this probe is monitoring.
Entry	The Entry number in the list of probes.
Flavor	Whether the probe type is Ethernet, History, or Alarm.
Status	The status of the probe–**Creating** (the probe is under creation), **Active** (the probe is Active), or **Inactive** (the probe is inactive).
Duration	Elapsed time (hours/minutes/seconds) since the last change in status.
System Resources	Amount of memory that has been allocated to this probe.

Release History

Release 7.1.1; command was introduced.

Related Commands

rmon probes	Enables or disables types of RMON probes.
show rmon events	Displays RMON logged events.

MIB Objects

```
ETHERSTATSTABLE
   etherStatsIndex
HISTORYCONTROLTABLE
   historyControlIndex
ALARMTABLE
   alarmIndex
```

show rmon events

Displays RMON events (actions that take place based on alarm conditions detected by the RMON probe).

show rmon events [*entry_number***]**

Syntax Definitions

entry_number	The entry number in the list of probes *(optional)*.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- To display a list of logged events, omit the *entry_number* from the command line.
- To display statistics for a particular event, include the *entry_number* in the command line.
- The **show rmon events** command displays the following information for all RMON Logged Events: Entry number, Time (hours/minutes/seconds) since the last change in status and Description (nature of the event).
- The **show rmon events** *entry_number* command displays the following information for a particular RMON Logged Event: Entry number, Time (hours/minutes/seconds) since the last change in status and Description (nature of the event).

Examples

```
-> show rmon events

Entry               Time               Description
---------+------------------+-----------------------------------------------------
1               00:08:00       etherStatsPkts.4008: [Falling trap] “Falling Event”
2               00:26:00       etherStatsCollisions.2008: “Rising Event”

-> show rmon events 2

Entry               Time               Description
---------+------------------+-----------------------------------------------------
2               00:26:00       etherStatsCollisions.2008: “Rising Event”
```

output definitions

Entry	The entry number in the list of probes.
Time	Time (hours, minutes, and seconds) since the last change in status.
Description	Description of the Alarm condition detected by the probe.

Release History

Release 7.1.1; command was introduced.

Related Commands

rmon probes	Enables or disables types of RMON probes.
show rmon probes	Displays RMON probes or a single RMON probe.

MIB Objects

```
EVENTTABLE
   eventIndex
```

50 Switch Logging Commands

This chapter includes descriptions for Switch Logging commands. These commands are used to configure parameters for the Switch Logging utility.

MIB information for the system commands is as follows:

Filename: ALCATEL-IND1-SYSTEM-MIB.mib
Module: alcatelIND1SystemMIB

A summary of the available commands is listed here.

swlog

Enables or disables switch logging. Switch logging allows you to view a history of various switch activities in a text format.

swlog {enable | disable | preamble | hash-time-limit *seconds* **| duplicate-detect | console level** *num* **}**

no swlog [preamble | duplicate-detect]

Syntax Definitions

enable	Enables the switch logging functionality.
disable	Disables the switch logging functionality.
preamble	Enables or disables the display of the preamble to the console.
hash-time-limit *seconds*	Configures the amount of elapsed time for an entry to no longer be considered a duplicate entry.
duplicate-detect	Enables or disables the duplicate detection capability.
console level *num*	The severity level filter keyword or numeric value for the application ID. *(see table for* **swlog appid** *command).*

Defaults

parameter	default
enable | disable	**enable**
preamble	**enable**
hash-time-limit *num*	**60 seconds**
duplicate-detect	**enable**
console level *num*	**6 (info)**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to enable or disable the **preamble** and **duplicate-detect** setting.
- The syslog preamble includes the level, appid, and timestamp that precedes the actual log messages.
- If duplicate entries are received within the configured **hash-time-limit,** only a single entry will be logged along with the number of times duplicated.
- Use the **swlog console level** command to set the switch logs of different levels to be displayed on the console.

Examples

```
-> swlog enable
-> swlog hash-time-limit 30
-> no swlog preamble
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1.R02; **gmt-time** parameter added.
Release 8.4.1; **gmt-time** parameter removed.

Related Commands

swlog appid	Defines the level at which switch logging information will be filtered for the specified application.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.
swlog console level	Allows to set the switch logs of different levels to be displayed on the console. All application events of defined level and lower are displayed on the console.

MIB Objects

```
systemSwitchLogging
   systemSwitchLoggingEnable
   systemSwitchLoggingPreamble
   systemSwitchLoggingHashAgeLimit
   systemSwitchLoggingDuplicateDetect
   systemSwitchLoggingConsoleLevel
   systemSwitchLoggingGmtTime
```

swlog syslog-facility-id

Specifies a facility ID that switch logging includes in the priority (PRI) section of the event message.

swlog syslog-facility-id {*facility_id* **|** *num***}**

Syntax Definitions

facility_id	A facility identification keyword. Current facility IDs are listed in the table below.
num	A numerical equivalent value for the facility ID. The range is 0–23. Current numeric equivalent values are listed in the table below.

Supported Facility IDs with Numerical Equivalents	
kernel - 0	**NTP - 12**
user - 1	**log-audit - 13**
mail - 2	**log-alert - 14**
system - 3	**clock2 - 15**
sec-auth1-2	**local0 - 16**
syslog - 5	**local1 - 17**
lptr - 6	**local2 - 18**
net-news - 7	**local3 - 19**
UUCP - 8	**local4 - 20**
clock1- 9	**local5 - 21**
sec-auth2 - 10	**local6 - 22**
FTP - 11	**local7 - 23**

Defaults

parameter	default
facility_id	**local0**
num	**16**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the ID name (**system**) or the numeric equivalent to specify the facility ID.

Examples

```
-> swlog syslog-facility-id system
-> swlog syslog-facility-id 3
-> swlog syslog-facility-id user
-> swlog syslog-facility-id 1
```

Release History

Release 8.3.1; command introduced.

Related Commands

swlog	Enables or disables switch logging.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLogging
   systemSwitchLoggingSysLogFacilityId
```

swlog appid

Defines the level at which switch logging information will be filtered for the specified application. All application events of the defined level and lower are captured.

swlog appid {all | *string***} {library {all |** *string***} | subapp {all |** *num***} | exclude {all |** *num***}} {disable | enable | level {***level* **|** *num***} [vrf** *num***]**

Syntax Definitions

string	An application or library identification keyword. Enter a question mark (?) on the command line to get a list of application or library IDs.
subapp *num*	A numerical equivalent value for the subapp ID. Enter a question mark (?) on the command line to get a list of subapp IDs.
exclude *num*	A numerical equivalent value for the subapp ID. Enter a question mark (?) on the command line to get a list of subapp IDs.
disable	Disables the logging of the associated application.
enable	Enables the logging of the associated application.
level *level* | *num*	The severity level filter keyword or numerical equivalent value for the application ID *(see table below)*. All switch logging messages of the specified level and lower will be captured. The severity level is a value assigned to the relative severity of the switch logging message. A lower value indicates messages that are more severe, a higher value indicates messages that are less severe.
vrf *num*	The VRF ID.

Supported Levels	Numeric Equivalents	Description
off	**0**	Disabled
alarm	**1**	Highest severity. The system is about to crash and reboot.
error	**2**	System functionality is reduced.
alert	**3**	A violation has occurred.
warning	**4**	A unexpected, non-critical event has occurred.
event	**5**	A clear readable customer event.
info	**6**	Any other non-debug message (default).
debug1	**7**	A normal event debug message.
debug2	**8**	A debug-specific message.
debug3	**9**	All debug messages.

Defaults

Default severity level is **info**.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **show swlog appid** command to display available registered applications.
- Specify the **event** severity level keyword to define the new event level at which switch logging information will be filtered for the specified application.

Examples

```
-> swlog appid all subid all enable
-> swlog appid mvrpNi subapp 1 level 8
-> swlog appid all supapp all level event
-> swlog appid all library all level event
-> swlog appid all exclude all level event
-> show swlog appid mvrpNi

Application Name                   : mvrpNi,

SubAppl ID Sub Application Name  Level         VRF Level
----------+--------------------+--------+------------------------------
         1 main                 error    VRF  1-64 info

-> swlog appid ?
              ^
              ALL <string>
              SWLOG PMD ChassisSupervisor flashManager MIP_GATEWAY
              ConfigManager capManCmm vc_licManager vcmCmm SSTIME SSAPP mrvld
              capManSig fabric portMgrCmm vfcm intfCmm dafcCmm linkAggCmm
              VlanMgrCmm ipmscmm pvlanCmm isis_spb_0 isisVc stpCmm AGCMM slCmm
              mirMonSFlowCmm ipv4 ipv6 ipsecSys ipsec tcamCmm qosCmm vstkCmm
              eoamCmm erpCmm NTP udpRelay remoteConfig AAA havlanCmm SES rmon
              WEBVIEW trapmgr radCli ldapClientCmm tacClientCmm healthCmm
              svcCmm lldpCmm udldCmm mpls saaCmm SNMP csEventMonitor
              bfdcmm mvrpCmm dhcp6r messageService dhcpv6Srv dhcpSrv grm
              bcdcmm lpCmm DG_CMM qmrCmm iprm_0 vrrp_0 ospf_0 flashManagerNI
              capManNi vcmNi portMgrNi bcd vfcn intfNi dafcNi linkAggNi
              VlanMgrNi stpNi erpNi vstkNi fdbmgr1 slNi healthNi ipni ip6ni
              mirMonSFlowNi tcamni qosNi ipmsni svcNi lldpNi udldNi
              bfdni mvrpNi AGNI DG_NI nipktrly loamNi eoamNi fdbmgr4 lpNi
              fdbmgr3

-> swlog appid udprelay library ?
                               ^
                               ALL <string>
                               plApi cslib pmdlib reactor capManLib SMAL BRUT
                               mcipc vfcLib vcmLib SysServices portmgrlibcmm
                               tcamlibcmm esmLib ipms_client ipmc_idx
                               mirApiLibCMM ipcmmLib qos mplscore routemap

-> swlog appid udprelay subapp ?
                              ^
                              ALL <num> <string>
                              1=main 2=dhcp-snooping 3=tcam
```

```
-> swlog appid udprelay exclude ?
                                ^
                                ALL <num> <string>
                                1=main 2=dhcp-snooping 3=tcam
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **exclude** parameter added.
Release 8.6.R1; **event** severity level keyword added.

Related Commands

swlog	Enables or disables switch logging.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.
swlog console level	Allows to set the switch logs of different levels to be displayed on the console. All application events of defined level and lower are displayed on the console.

MIB Objects

```
systemSwitchLogging
   systemSwitchLoggingAppName
   systemSwitchLoggingLibraryName
   systemSwitchLoggingLevel
```

swlog output

Enables or disables switch logging output to the console, file, data socket (remote session), or external syslog server.

swlog output {tty {enable | disable} | console | flash | socket {*ip_address* **|** *ipv6Address* **|** *domain_name***} [tls] [remote command-log] [vrf-name** *name***]}**

no swlog output {console | flash | socket [*ip_address* **|** *ipv6Address* **|** *domain_name***]}**

Syntax Definitions

tty enable	Enables switch logging to a connected Telnet session.
tty disable	Disables switch logging to a connected Telnet session.
console	Specifies console output. When enabled, switch logging output is printed to the user console.
flash	Specifies /flash file output. When enabled, switch logging output is printed to a file in the switch's /flash file system.
socket	Specifies data socket output. When enabled, switch logging output is printed to a remote session.
ip_address	The IPv4 address for the remote session host.
ipv6Address	The IPv6 address for the remote session host.
domain_name	A Fully Qualified Domain Name (FQDN) for the remote session host. Specify a domain name up to 128 characters in length.
tls	Enables or disables syslog over TLS.
remote command-log	Enables command logging to a remote session host.
name	Specifies the VRF to be used to access the remote syslog server.

Defaults

parameter	default
console | **flash** | **socket**	**flash** and **console**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable one or more configured output IP addresses.
- This command can also be used on the secondary CMM.
- Use the **socket** keyword to send output to a syslog server, followed by the IP address or FQDN of the remote host. Up to 12 servers can be configured. When an FQDN is specified, the switch will resolve the domain name to an IP address. Make sure the domain name maps to a valid and reachable IP address.

- Syslog over TLS:
  - Remote command log will not work when syslog over TLS is enabled.
  - VRF cannot be used to access the syslog server when syslog over TLS is enabled.
  - In OmniSwitch 9900 only CMM swlog is transferred to the external syslog server over TLS.
  - Dying Gasp syslog messages are not captured in syslog over TLS.
  - Use the **no** form of the command to disable syslog over TLS.
- VRF name must either be 'default' or a pre-defined VRF (user-defined).

Examples

```
-> swlog output console
-> no swlog output flash
-> swlog output socket 14.1.1.1
-> swlog output socket 14.1.1.1 remote command-log
-> swlog output socket 14.1.1.1 vrf-name vrf1
-> no swlog output socket 14.1.1.1

-> swlog output socket upam.omnivista.com
-> swlog output socket upam.omnivista.com remote command-log
-> swlog output socket upam.omnivista.com vrf-name vrf1
-> no swlog output socket upam.omnivista.com
-> swlog output socket opendaylight.com
ERROR: DNS lookup failed, unknown host opendaylight.com
-> swlog output socket 192.168.120.140 tls
-> swlog output socket 2001::1 tls
-> no swlog output socket 2001::1
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **vrf-name** parameter added.
Release 8.3.1; **remote command-log** parameter added.
Release 8.5R1; *domain_name* parameter option added.
Release 8.6R1; **tls** parameter added.

Related Commands

swlog	Enables or disables switch logging.
swlog appid	Defines the level at which switch logging information will be filtered for the specified application.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLogging
   systemSwitchLoggingTty
   systemSwitchLoggingFlash
   systemSwitchLoggingSocket
   systemSwitchLoggingSocketIpAddr
   systemSwitchLoggingConsole
systemSwitchLoggingHostTable
   systemSwitchLoggingHostIpAddr
   systemSwitchLoggingHostPort
   systemSwitchLoggingHostStatus
   systemSwitchLoggingHostUserCommandHost
   systemSwitchLoggingHostVrfName
systemSwitchLoggingHostDnTable
   systemSwitchLoggingHostDnName
   systemSwitchLoggingHostDnPort
   systemSwitchLoggingHostDnUserCommandHost
   systemSwitchLoggingHostDnVrfName
   systemSwitchLoggingHostDnStatus
   systemSwitchLoggingHostTls
```

swlog output flash-file-size

Configures the size of the switch logging file.

swlog output flash-file-size *kilobytes*

Syntax Definitions

kilobytes	The size of the switch logging file in kilobytes. The range is 125–12500.

Defaults

parameter	default
kilobytes	1250

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **show hardware-info** command to determine the amount of available flash memory.
- This command can also be used on the secondary CMM.

Examples

```
-> swlog output flash-file-size 256
```

Release History

Release 7.1.1; command was introduced.

Related Commands

swlog advanced	Clears the files that store switch logging data.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLogging
   systemSwitchLoggingFileSize
```

swlog advanced

Enable or disable switch logging in RFC5424 format.

swlog advanced {enable | disable}

Syntax Definitions

enable	Enable switch logging in RFC5424 format.
disable	Disable switch logging in RFC5424 format.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- By default, the switch logs the messages in BSD syslog format (RFC3164) to files and remote syslog servers.
- When switch logging RFC5424 format is enabled, the old RFC3164 syslog messages are reformatted to comply with the RFC5424 before writing to files or sending to remote syslog servers.

Examples

```
-> swlog advanced enable
-> swlog advanced disable
```

Release History

Release 8.4.1; command introduced.

Related Commands

show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingSyslogProtocol
```

swlog size-trap-threshold

Configures the threshold limit of the storage space used for swlog record storage. When the storage reaches the configured threshold limit a notification is displayed in the swlog message.

swlog size-trap-threshold *threshold*

Syntax Definitions

threshold	The percentage of storage space to be set as threshold limit. The valid range is 50–90.

Defaults

parameter	default
threshold	90

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to configure the threshold limit of the storage space used for swlog record storage.
- Use the **swlog clear** command to clear the files that store switch logging data.

Examples

```
-> swlog size-trap-threshold 90
```

Release History

Release 8.4.1; command introduced.

Related Commands

swlog clear	Clears the files that store switch logging data.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingSizeTrapThreshold
```

swlog clear

Clears the files that store switch logging data.

swlog clear [all]

Syntax Definitions

all	Clears all the contents of the switch log file.

Defaults

By default, the contents of the switch log file is cleared but the event logs are retained.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command when the switch logging display is too long due to some of the data being old or out of date.
- This command can also be used on the secondary CMM.
- To clear all the contents including the event log use the "**all**" parameter with swlog clear command.

Examples

```
-> swlog clear
-> swlog clear all
```

Release History

Release 7.1.1; command was introduced.
Release 8.6R2; **all** parameter added.

Related Commands

swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLogging
   systemSwitchLoggingClear
```

show log swlog

Displays stored switch logging information.

show log swlog

show log swlog [timestamp *mm/dd/yyyy hh:mm:ss***] [slot** *num***]**

Syntax Definitions

mm/dd/yyyy hh:mm:ss	Specify the starting time for the switch logging information to be displayed. Use the format ***mm/dd/yyyy hh:mm:ss*** where ***mm*** represents the month, ***dd*** is the day, ***yyyy*** is the year, ***hh*** is the hour, ***mm*** is the minutes and ***ss*** is the seconds. Use four digits to specify the year.
num	The slot number to display the logging information for. *Currently not supported*.

Default

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the switch logging display is too long, you may use the **swlog advanced** command to clear all of the switch logging information.
- The use of **grep** and the **timestamp** parameter can be used to filter the log files.
- When the switch is in ASA enhanced mode, both user name and password is prompted to view the SWLOG data using **show log swlog** command. Only those users who provide the valid ASA credentials are allowed to view the data. For more information on Authenticated Switch Access - Enhanced Mode mode, refer to the “Managing Switch Security” chapter in *OmniSwitch AOS Release 8 Switch Management Guide.*

Examples

```
-> show log swlog timestamp 09/30/2011 13:27:00
Displaying file contents for '/flash/swlog.6'
Displaying file contents for '/flash/swlog.5'
<output truncated>

Sep 30 13:27:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!

-> show log swlog | grep ChassisSupervisor
Displaying file contents for '/flash/swlog.6'
Displaying file contents for '/flash/swlog.5'
<output truncated>
```

```
Sep 28 13:25:15 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!

Sep 30 13:26:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!

Sep 30 13:27:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!
```

When the switch is in ASA enhanced mode, both user name and password is prompted to view the SWLOG data using **show log swlog** command.

```
-> show log swlog
Username: test
Password:   *******
```

show log swlog | grep error and **show log swlog | grep more** commands are not supported in enhanced mode.

Release History

Release 7.1.1; command was introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid	Adds or removes a filter level for a specified subsystem.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
swlog advanced	Clears the files that store switch logging data.
show swlog	Displays switch logging information.

MIB Objects

```
N/A
```

show swlog

Displays switch logging information (for example, switch logging status, log devices, application IDs with non-default severity level settings).

show swlog [library | appid {all | *string***} | dying-gasp-station]**

Syntax Definitions

library	Displays the entire library for all application IDs.
string	The name of the application ID to display. Enter a question mark (?) on the command line to get a list of application IDs.
dying gasp-station	Displays switch logging information for Dying Gasp entries.

Defaults

By default, the switch logging configuration for the switch is displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> show swlog
Operational Status                : Running,
File Size per file                : 1250 Kbytes,
Log Device 1                      : console flash socket,
Log Device 2                      : ipaddr 10.2.2.1 remote command-log,
Syslog FacilityID                 : local0(16),
Hash Table entries age limit      : 60 seconds,
Switch Log Preamble               : Enabled,
Switch Log Debug                  : Disabled,
Switch Log Duplicate Detection    : Enabled,
Console Display Level             : debug1,
RFC5424 Format Logging            : Enabled,
Swlog Threshold                   : 90 percent
Syslog over TLS                   : Enabled

-> show swlog appid udprelay
Operational Status                : Running,
File Size per file                : 1500 Kbytes,
Log Device 1                      : console flash,
Log Device 2                      : upam.omnivista.com remote command-log,
Syslog FacilityID                 : local0(16),
Hash Table entries age limit      : 60 seconds,
Switch Log Preamble               : Enabled,
Switch Log Debug                  : Disabled,
Switch Log Duplicate Detection    : Enabled,
Console Display Level             : debug1,
```

```
RFC5424 Format Logging             : Disabled,
Application Name(id)               : udpRelay(38),
SubAppl ID Sub Application Name  Level         VRF Level
----------+--------------------+--------+-----------------------------
         1 main                 info     VRF  1-1024 info
         2 dhcp-snooping        info     VRF  1-1024 info
         3 tcam                 info     VRF  1-1024 info

-> show swlog dying-gasp-station
Operational Status                 : Running,
Log Device                         : console flash,
Log Device                         : ipaddr 10.2.2.1 remote command-log,
Syslog FacilityID                  : local0(16)
```

output definitions

Operational Status	Displays whether switch logging is enabled or disabled.
File Size per file	The maximum file size of the switch log file.
Log Device	Which devices are the switch log messages being sent to.
Log Device	Which devices are the switch log messages being sent to.
Syslog FacilityID	The Facility ID value that is included in the priority (PRI) section of the event messages.
Hash Table entries age limit	The elapsed time for duplicate entries.
Switch Log Preamble	Status of displaying message preamble on console.
Switch Log Debug	Status of swlog debug.
Switch Log Duplicate Detection	Status of duplicate detection.
Console Display Level	The console severity level.
RFC5424 Format Logging	Displays if switch logging in RFC5424 format is enabled or disabled.
Swlog Threshold	Displays the configured threshold limit for swlog record storage.
Syslog over TLS	Displays the operational status of syslog over TLS.
Application Name(id)	The subsystem information for the Application ID.

```
-> show swlog appid ?
                   ^
                   ALL <string>
                   SWLOG PMD ChassisSupervisor flashManager MIP_GATEWAY
                   ConfigManager capManCmm vc_licManager vcmCmm SSTIME SSAPP
                   mrvld capManSig fabric portMgrCmm vfcm intfCmm dafcCmm
                   linkAggCmm VlanMgrCmm ipmscmm pvlanCmm isis_spb_0 isisVc
                   stpCmm AGCMM slCmm mirMonSFlowCmm ipv4 ipv6 ipsecSys ipsec
                   tcamCmm qosCmm vstkCmm eoamCmm erpCmm NTP udpRelay
                   remoteConfig AAA havlanCmm SES rmon WEBVIEW trapmgr radCli
                   ldapClientCmm tacClientCmm healthCmm svcCmm lldpCmm udldCmm
                   mpls saaCmm SNMP csEventMonitor bfdcmm mvrpCmm
                   dhcp6r messageService dhcpv6Srv dhcpSrv grm bcdcmm lpCmm
                   DG_CMM qmrCmm iprm_0 vrrp_0 ospf_0 flashManagerNI capManNi
                   vcmNi portMgrNi bcd vfcn intfNi dafcNi linkAggNi VlanMgrNi
                   stpNi erpNi vstkNi fdbmgr1 slNi healthNi ipni ip6ni
                   mirMonSFlowNi tcamni qosNi ipmsni svcNi lldpNi udldNi
                   bfdni mvrpNi AGNI DG_NI nipktrly loamNi eoamNi fdbmgr4 lpNi
```

```
fdbmgr3
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **dying-gasp-station** parameter added.
Release 8.3.1.R02; **GMT time logging** field added.
Release 8.4.1; **GMT time logging** field replaced with **RFC5424 Format Logging**. **Swlog Threshold**.
Release 8.6R1; **Syslog over TLS** field added in show swlog output.

Related Commands

swlog	Enables or disables switch logging.
swlog syslog-facility-id	Configures the value of the facility ID that switch logging includes in the priority (PRI) section of the event message.
swlog appid	Defines the level at which switch logging information will be filtered for the specified application.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
swlog output flash-file-size	Configures the size of the switch logging file.
swlog size-trap-threshold	Configures the threshold limit of the storage space used for swlog record storage.
show log swlog	Displays stored switch logging information from flash.
show log events	Displays customer event logs on the switch.
show log events output	Captures all event log to a specified file name on the switch.

MIB Objects

```
systemSwitchLogging
   systemSwitchLoggingEnable
   systemSwitchLoggingPreamble
   systemSwitchLoggingHashAgeLimit
   systemSwitchLoggingDuplicateDetect
   systemSwitchLoggingConsoleLevel
   systemSwitchLoggingGmtTime
   systemSwitchLoggingSysLogFacilityId
   systemSwitchLoggingAppName
   systemSwitchLoggingLibraryName
   systemSwitchLoggingLevel
   systemSwitchLoggingTty
   systemSwitchLoggingFlash
   systemSwitchLoggingSocket
   systemSwitchLoggingSocketIpAddr
   systemSwitchLoggingConsole
   systemSwitchLoggingFileSize
   systemSwitchLoggingSyslogProtocol
   systemSwitchLoggingSizeTrapThreshold
systemSwitchLoggingHostTable
   systemSwitchLoggingHostIpAddr
   systemSwitchLoggingHostPort
   systemSwitchLoggingHostStatus
   systemSwitchLoggingHostUserCommandHost
```

```
   systemSwitchLoggingHostVrfName
   systemSwitchLoggingHostTls
systemSwitchLoggingDgHostTable
   systemSwitchLoggingDgHostIndex
   systemSwitchLoggingDgHostIpType
   systemSwitchLoggingDgHostIpAddr
```

swlog console level

Allows to set the switch logs of different levels to be displayed on the console. All application events of defined level and lower are displayed on the console.

swlog console level {*num* **| alarm | alert | debug1 | debug2 | debug3 | error | info | off | warning }**

Syntax Definitions

console level *num*	The severity level filter keyword or numeric value for the application ID. *(see table for* **swlog appid** *command).*
alarm	Sets the log level to display highest severity. (The system is about to crash and rebbot)
alert	Sets the log level to display on console when a violation has occured.
debug1	Sets the log level to display normal event debug message to be displayed on console.
debug2	Sets the log level to display a debug-specific message to be displayed on console.
debug3	Sets the log level to display all debug messages on the console.
error	Sets the log level to display on console when system functionality is reduced.
info	Sets the log level to display any other non-debug message on the console.
off	Sets the log level as disabled. No logs are displayed on the console.
warning	Sets the log level to display on console when an unexpected, non-critical event has occurred.

Defaults

parameter	default
console level *num*	**6 (info)**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **show swlog** command to display the console display level.

Examples

```
-> swlog console level 5
-> swlog console level info
```

Release History

Release 7.1.1; command was introduced.

Related Commands

swlog appid	Defines the level at which switch logging information will be filtered for the specified application.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.
show log events	Displays customer event logs on the switch.
show log events output	Captures all event log to a specified file name on the switch.

MIB Objects

```
systemSwitchLogging
   systemSwitchLoggingConsoleLevel
```

show log events

Displays customer event logs on the switch.

show log events

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display customer event logs.

Examples

```
-> show log events
2019 Apr 28 19:17: 8.83  : CMM : ChassisSupervisor : chassisTrapsAlert - CERTIFY w/
FLASH SYNCHRO process started
2019 Apr 28 19:17:32.697 : CMM : ChassisSupervisor : chassisTrapsAlert - CERTIFY
process completed successfully
2019 Apr 28 19:21:33.154 : CMM : ChassisSupervisor : chassisTrapsAlert - ACTIVATE
process scheduled
2019 Apr 28 19:21:57.462 : CMM : ChassisSupervisor : System Reboot
2019 Apr 28 19:25:25.302 : CMM : ChassisSupervisor : chassisTrapsAlert - Power
supply is OK
2019 Apr 28 19:25:25.303 : CMM : ChassisSupervisor : The switch was restarted by
the user
2019 Apr 28 19:25:25.304 : CMM : ChassisSupervisor : chassisTrapsAlert - CMM
startup completed
```

output definitions

The log output is in the following format: <SWLOG TIMESTAMP> : <CMM>/<NI> : <MODULE_NAME> : <LOG_DESCRIPTION>

Release History

Release 8.6R1; command was introduced.

Related Commands

show log events output	Captures all event log to a specified file name on the switch.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

N/A

show log events output

Captures all event log to a specified file name on the switch.

show log events output *filename*

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to capture all event log to a filename.
- All the logs related to customer events will be appended “CUSTLOG” to the prefix to differentiate events from normal debug logs.

Examples

```
-> show log events output /flash/myevents
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show log events	Displays customer event logs on the switch.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

N/A

51 Health Monitoring Commands

The Health Monitoring function monitors the consumable resources of the switch (for example, bandwidth usage, CPU usage) and provides a single integrated resource for a Network Management System (NMS). This function monitors the switch, and at fixed intervals, collects the current values for each resource being monitored. Users specify resource threshold limits and traps are sent to an NMS if a value falls above or below a user-specified threshold.

The Health Monitoring commands comply with RFC1212.

MIB information for the Health Monitoring commands is as follows:

Filename: ALCATEL-IND1-HEALTH-MIB.mib
Module: alcatelIND1HealthMonitorMIB

A summary of the available commands is listed here:

health threshold

Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, CPU usage, and flash usage.

Input traffic, output/input traffic, memory usage, and CPU usage thresholds specify the maximum percentage for each resource that may be consumed before a trap is sent to the user.

health threshold {rx *percent* **| txrx** *percent* **| memory** *percent* **| cpu** *percent* **| flash** *percent***}**

Syntax Definitions

rx	Specifies the maximum input (RX) traffic threshold.
txrx	Specifies the maximum output/input (TX/RX) traffic threshold.
memory	Specifies the maximum RAM memory usage threshold.
cpu	Specifies the maximum CPU usage threshold.
flash	Specifies the maximum flash usage threshold.
percent	The new threshold value, in percent, for the corresponding resource (**rx**, **txrx**, **memory**, **cpu, flash**). The valid range is 1–100.

Defaults

parameter	default
percentage	80

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When a resource falls back below the configured threshold, an additional trap is sent to the user. This indicates that the resource is no longer operating beyond its configured threshold limit.
- Changing a threshold value sets the value for all levels of the switch (the switch, module, and port). You cannot set different threshold values for each level.
- For detailed information on each threshold type, refer to page 51-5, or refer to the chapter titled “Diagnosing Switch Problems” in the *OmniSwitch AOS Release 8 Network Configuration Guide*.
- To view the current health threshold values, use the **show health configuration** command.

Examples

```
-> health threshold rx 85
-> health threshold txrx 55
-> health threshold memory 95
-> health threshold cpu 85
```

Release History

Release 7.1.1; command introduced.

Related Commands

show health configuration	Displays the current health threshold settings.

MIB Objects

```
HealthThreshInfo
   healthThreshDeviceRxLimit
   healthThreshDeviceTxRxLimit
   healthThreshDeviceMemoryLimit
   healthThreshDeviceCpuLimit
   healthThreshFlashLimit
```

health interval

Configures the sampling interval between health statistics checks. The sampling interval is the time interval between polls of the consumable resources of the switch to see if it is performing within set thresholds.

health interval *seconds*

Syntax Definitions

seconds	Sampling interval (in seconds). Valid entries are 10, 12, 15, 20, 30.

Defaults

parameter	default
seconds	10

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Decreasing the polling interval may impact switch performance.

Examples

```
-> health interval 20
```

Release History

Release 7.1.1; command introduced.

Related Commands

show health	Displays the current health sampling interval.

MIB Objects

```
HealthThreshInfo
   healthSamplingInterval
```

show health configuration

Displays current health configuration settings.

show health configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show health configuration
Rx Threshold                  = 80,
TxRx Threshold                = 80,
CPU Threshold                 = 80,
Memory Threshold              = 80,
Flash Threshold               = 80,
Sampling Interval (Secs)      = 10
```

output definitions

Rx Threshold	The current device input (RX) threshold. This value displays the maximum percentage of total bandwidth allowed for *incoming traffic* on the switch. The total bandwidth is defined as the Ethernet port capacity for all NI modules currently operating in the switch, in Mbps. For example, a chassis with 48 100Base-T Ethernet ports installed has a total bandwidth of 4800 Mbps. The default value is 80 percent and can be changed using the **health threshold** command.
TxRx Threshold	The current device output/input (TX/RX) threshold. This value displays the maximum percentage of total bandwidth allowed for *all incoming and outgoing traffic*. As with the RX threshold described above, the total bandwidth is defined as the Ethernet port capacity for all the NI modules currently operating in the switch, in Mbps. The default value is 80 percent and can be changed using the **health threshold** command.
CPU Threshold	Displays the current CPU usage threshold. CPU usage refers to the total amount of CPU processor capacity currently used by switch applications. The default value is 80 percent and can be changed using the **health threshold** command.

output definitions (continued)

Memory Threshold	Displays the current memory usage threshold. Memory usage refers to the total amount of RAM memory currently used by switch applications. The default value is 80 percent and can be changed using the **health threshold** command.
Flash Threshold	Displays the current flash usage threshold. The default value is 80 percent and can be changed using the **health threshold** command.
Sampling Interval	Displays the sampling interval time period in seconds. Sampling interval can be changed using the **health interval** command.

Release History

Release 7.1.1; command introduced.

Related Commands

health threshold	Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage and CPU usage.
health interval	Configures the sampling interval between health statistics checks.

MIB Objects

```
HealthThreshInfo
   healthThreshDeviceRxLimit
   healthThreshDeviceTxRxLimit
   healthThreshDeviceMemoryLimit
   healthThreshDeviceCpuLimit
```

show health

Displays the health statistics for the switch. Statistics are displayed as percentages of total resource capacity and represent data taken from the last sampling interval.

show health [port *chassis/slot/port* **| slot** *chassis/slot***[-***slot2***]] [statistics]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	To view a specific port, enter the slot and port number (3/1) along with the **port** keyword (port 3/1).
*slot***[-***slot2***]**	To view a series of slots, enter the range of slot numbers along with the **slot** keyword (1-10).
statistics	Optional command syntax. It displays the same information as the **show health** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If no slot or port information is specified, the aggregate health statistics for all ports is displayed.

Examples

```
-> show health
CMM                  Current    1 Min    1 Hr   1 Day
Resources                       Avg      Avg    Avg
-------------------+---------+-------+------+-------
CPU                      0      0       0      0
Memory                  30      30     24     24

-> show health port 1/1/24
Port 1/1/24     Limit  Current  1 Min   1 Hr  1 Day
Resources              Avg      Avg     Avg
---------------+-----+--------+-------+-----+-------
Receive          80     01       01      01    01
Transmit/Receive 80     01       01      01    01
```

output definitions

Receive	Traffic received by the switch.
Transmit/Receive	Traffic transmitted and received by the switch.
Memory	Switch memory.
CPU	Switch CPU.

output definitions (continued)

Limit	Currently configured device threshold levels.
Curr	Current device bandwidth usage.
1 Min Avg	Average device bandwidth usage over a 1-minute period.
1 Hr Avg	Average device bandwidth usage over a 1-hour period.
1 Hr Max	Maximum device bandwidth usage over a 1-hour period (the maximum of the 1 minute averages).

Release History

Release 7.1.1; command introduced.
Release 8.5R1; **Limit** output field included.

Related Commands

show health all	Displays health statistics for a specified resource on *all* NIs currently operating in the chassis.

MIB Objects

```
healthModuleTable
   healthModuleSlot
   healthModuleRxLatest
   healthModuleRx1MinAvg
   healthModuleRx1HrAvg
   healthModuleRx1HrMax
   healthModuleRxTxLatest
   healthModuleRxTx1MinAvg
   healthModuleRxTx1HrAvg
   healthModuleRxTx1HrMax
   healthModuleMemoryLatest
   healthModuleMemory1MinAvg
   healthModuleMemory1HrAvg
   healthModuleMemory1HrMax
   healthModuleCpuLatest
   healthModuleCpu1MinAvg
   healthModuleCpu1HrAvg
   healthModuleCpu1HrMax
```

show health all

Displays health statistics for a specified resource on all *active NI modules* installed in the chassis.

show health all {memory | cpu | rx | txrx}

Syntax Definitions

memory	Displays the RAM memory health statistics for all active NI modules in the switch.
cpu	Displays the CPU health statistics for all active NI modules.
rx	Displays the health statistics for traffic *received* on all active NI modules.
txrx	Displays the health statistics for traffic both *transmitted and received* on all active NI modules.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show health all memory

* - current value exceeds threshold

                         1 Min  1 Hr  1 Hr
Memory              Curr   Avg    Avg   Max
-----------------+-------+------+------+-----
01                   40     40    40    40
02                   40     40    40    40
03                   40     40    40    40
04                   40     40    40    40
05                   40     40    40    40
06                   40     40    40    40
07                   40     40    40    40
13                   40     40    40    40
```

output definitions

Memory (Cpu, TXRX, RX)	A list of all currently-active NI modules (i.e., active slots) on the switch. The column header corresponds with the resource keyword entered. For example, if **show health all cpu** is entered, **Cpu** is used as the column header.
Curr	Current usage of the resource on the corresponding slot, in percent (the amount of the total resource bandwidth actually being used by the switch applications).
1 Min Avg	Average usage of the resource on the corresponding slot over a one minute period.
1 Hr Avg	Average usage of the resource on the corresponding slot over a one hour period.
1 Hr Max	The highest average hourly usage for the resource on the corresponding slot.

Release History

Release 7.1.1; command introduced.

Related Commands

show health	Displays the health statistics for the switch.
health threshold	Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, and CPU usage.

MIB Objects

```
healthModuleTable
   healthModuleSlot
   healthModuleRxLatest
   healthModuleRx1MinAvg
   healthModuleRx1HrAvg
   healthModuleRx1HrMax
   healthModuleRxTxLatest
   healthModuleRxTx1MinAvg
   healthModuleRxTx1HrAvg
   healthModuleRxTx1HrMax
   healthModuleMemoryLatest
   healthModuleMemory1MinAvg
   healthModuleMemory1HrAvg
   healthModuleMemory1HrMax
   healthModuleCpuLatest
   healthModuleCpu1MinAvg
   healthModuleCpu1HrAvg
   healthModuleCpu1HrMax
```

52 Ethernet OAM Commands

Service provider networks are large and complex with a wide user base, and they often involve different operators that must work together in order to provide end-to-end services to enterprise customers. Operations, Administration, and Maintenance (OAM) provides service assurance over a converged network that service providers are looking for in an Ethernet network. Ethernet OAM addresses areas such as availability, mean time to repair and more. Ethernet OAM focuses on two main areas that are most in need by service providers and are rapidly evolving in the standards bodies, Service OAM and Link OAM. These two OAM protocols have unique objectives but are complementary to each other. Service OAM provides monitoring and troubleshooting of end-to-end Ethernet service instances, while Link OAM allows a provider to monitor and troubleshoot an individual Ethernet link.

MIB information for the Ethernet OAM commands is as follows:

Filename: Alcatel-IND1-ETHERNET-OAM-MIB.mib
Module: alcatelIND1EoamMIB

Filename: IEEE8021-CFM-MIB.mib
Module: ieee8021CfmMib

A summary of the available commands is listed here:

EthOAM vlan Configuration Commands	**ethoam vlan**
EthOAM Domain Configuration Commands	**ethoam domain** **ethoam domain mhf** **ethoam domain id-permission**
EthOAM Management Association Configuration Commands	**ethoam association** **ethoam association primary vlan** **ethoam association mhf** **ethoam association id-permission** **ethoam association ccm-interval** **ethoam association endpoint-list** **clear ethoam statistics**
EthOAM Default-Domain Configuration Commands	**ethoam default-domain level** **ethoam default-domain mhf** **ethoam default-domain id-permission** **ethoam default-domain primary-vlan**
EthOAM Management Point Configuration Commands	**ethoam endpoint** **ethoam endpoint admin-state** **ethoam endpoint rfp** **ethoam endpoint ccm** **ethoam endpoint priority** **ethoam endpoint lowest-priority-defect**

EthOAM Loopback and Linktrace Commands	**ethoam linktrace** **ethoam loopback**
EthOAM Timer Configuration Commands	**ethoam fault-reset-time**
EthOAM Performance Monitoring Configuration Commands	**ethoam one-way-delay** **ethoam two-way-delay** **clear ethoam**
EthOAM Show Commands	**show ethoam** **show ethoam domain** **show ethoam domain association** **show ethoam domain association end-point** **show ethoam default-domain configuration** **show ethoam default-domain** **show ethoam remote-endpoint domain** **show ethoam cfmstack** **show ethoam linktrace-reply** **show ethoam linktrace-tran-id** **show ethoam vlan** **show ethoam statistics** **show ethoam config-error** **show ethoam one-way-delay** **show ethoam two-way-delay**

ethoam vlan

Creates an association between Primary VID and Non-Primary VID(s).

ethoam vlan *vlanid_list* **primary-vlan** *vlan_id*

no ethoam vlan *vlanid_list*

Syntax Definitions

vlanid_list	A list of VLAN Identifiers (e.g.,'10 30-40' or '10').
vlan_id	VLAN Identifier (e.g., '20').

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Each VLAN ID specified must be created before creating any association.
- Each VLAN ID specified must be between 1 and 4094.
- Each VLAN ID specified must be static.
- A Non-Primary VID can only be associated with single Primary VID.
- Once Primary VID is associated with Non-Primary VID, then it can not be configured as Non-Primary VID. Its association must be removed before it is configured as Non-Primary VID.
- This CLI shall trigger Automip for this VLAN, if either 'mhf' is enabled for MA or default-MD with primary VLAN same as the primary VLAN of this VLAN.
- If the VLAN is deleted using VLAN CLI (no vlan *vlan_id*) and VLAN is non-primary, then the entry for this VLAN in the VLAN table will be deleted. This shall in turn delete all MEPs and MIPs associated with it. If the deleted VLAN is primary VLAN, then all its associated VLAN entries in the VLAN table shall be deleted. This shall in turn delete all MAs on this deleted VLAN.
- Use the **no** form of this command to dissociate Primary VID from the Non-Primary VID(s).

Examples

```
-> ethoam vlan 10 primary-vlan 20
-> ethoam vlan 11-15 primary-vlan 20
-> ethoam vlan 30 40-50 primary-vlan 20
-> no ethoam vlan 10
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam vlan	Displays the Ethernet OAM statistics of all the Management Domains configured on the bridge.

MIB Objects

```
dot1agCfmVlanTable
   dot1agCfmVlanComponentId
   dot1agCfmVlanVid
   dot1agCfmVlanPrimaryVid
   dot1agCfmVlanRowStatus
```

ethoam domain

Creates an Ethernet domain with a specific name.

ethoam domain *md_name* **format {none | dnsname | mac-address-uint | string} level** *num*

no ethoam domain *name*

Syntax Definitions

md_name	Specifies the domain name.
none	This format is supported for the inter-op with ITU-T Y.1731.
dnsname	Domain Name like string, globally unique text string derived from a DNS name.
mac-address-unit	MAC address + 2-octet (unsigned) integer.
string	Character String.
num	MD Level and it ranges from 0 to 7.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Maximum domain length is 43.
- Use format as ‘none’ for inter-op with ITU-T Y.1731.
- Domain name is unique in a system.
- Deletion of MD shall result in the deletion of all MAs, MEPs, and MIPs configured in the MD.

Examples

```
-> ethoam domain MD format none level 3
-> ethoam domain MD1 format string level 4
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam	Displays the information of all the Management Domains (MD) configured on the bridge.
show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
   dot1agCfmMdFromat
   dot1agCfmMdLevel
```

ethoam domain mhf

Configure the Message Handling Function (MHF) value for MD entry.

ethoam domain *md_name* **mhf {none** | **explicit** | **default}**

Syntax Definitions

md_name	Specifies the domain name used while creating the management domain for which this management association is created.
none	No MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.
default	MHFs can be created.

Defaults

parameter	default
none | explicit | default	**none**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Domain must be created before it is modified.

Examples

```
-> ethoam domain MD mhf default
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam	Displays the information of all the Management Domains (MD) configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
   dot1agCfmMdMhfCreation
```

ethoam domain id-permission

Configures the ID-permission value for MD entry.

ethoam domain *md_name* **id-permission {none | chassisid}**

Syntax Definitions

md_name	Specifies the domain name used while creating the management domain for which this management association is created.
none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.System name shall be filled as Chassis ID.

Defaults

parameter	default
none | chassisid	**none**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Domain must be created before it is modified.

Examples

```
-> ethoam domain MD id-permission chassisid
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.
show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
   dot1agCfmMdIdPermission
```

ethoam association

Creates Maintenance Association (MA) entry.

ethoam association *ma_name* **format {vpnid | unsignedint | string | primaryvid | icc-based} domain** *md_name*

no ethoam association *ma_name* **domain** *md_name*

Syntax Definitions

ma_name	Association name for the created Ethernet OAM Association.
vpnid	As specified in RFC 2685 VPN ID.
unsignedint	2-octet unsigned integer.
string	Character String.
primaryvid	Primary VLAN ID (12 bits represented in a 2-octet integer).
icc-based	This format is supported for inter-op with ITU-T.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Maximum association name is name 44 minus the length of its domain name.
- Use format as ‘icc-based’ to inter-op with ITU-T Y.1731.
- Domain must be created before the creation of MA.
- VLAN must be created before the creation of MA.
- VLAN specified must be a primary VID.
- Deletion of MA shall result in the deletion of MIPs and MEPs (on primary and non-primary VLAN) configured in it.
- Use the **no** form of the command to delete the Maintenance Association (MA) entry.

Examples

```
-> ethoam association MA format string domain MD
-> no ethoam association MA format string domain MD
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMaNetTable
   dot1agCfmMaNetFormat
   dot1agCfmMaNetName
   dot1agCfmMaNetRowStatus
dot1agCfmMaCompTable
   dot1agCfmMaComponentId
   dot1agCfmMaCompPrimaryVid
   dot1agCfmMaCompRowStatus
```

ethoam association primary vlan

Creates a primary VLAN for the Maintenance Association (MA) entry.

ethoam association *ma_name* **domain** *md_name* **primary-vlan** *vlan_id*

no ethoam association *ma_name* **domain** *md_name* **primary-vlan** *vlan_id*

Syntax Definitions

ma_name	Association name for the created Ethernet OAM Association.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
vlan_id	Primary VLAN Identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Domain must be created before the creation of MA.
- VLAN ID specified must be between 1 and 4094.
- Deletion of MA shall result in the deletion of MIPs and MEPs (on primary and non-primary VLAN) configured in it.
- Use the **no** form of the command to remove the Primary VLAN association.

Examples

```
-> ethoam association MA domain MD primary-vlan 100
-> no ethoam association MA domain MD primary-vlan 100
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMaCompTable
   dot1agCfmMaComponentId
   dot1agCfmMaCompPrimaryVid
   dot1agCfmMaCompRowStatus
```

ethoam association mhf

Configures the MIP Half Function (MHF) value for MA Entry.

ethoam association *ma_name* **domain** *md_name* **mhf {none | default | explicit | defer}**

Syntax Definitions

ma_name	Association name for the created Ethernet OAM Association.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.
defer	The creation of MHFs is determined by the corresponding MD object 'dot1agCfmMdMhfCreation'.

Defaults

parameter	default
none | explicit | default | defer	**defer**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- MA must be created before it is modified.
- On modification of 'mhf' for any MA, Automip shall also be invoked for all VLANS associated with this primary VID.

Examples

```
-> ethoam association MA domain MD mhf-creation defer
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.
show ethoam default-domain	Displays the information of the default MA.

MIB Objects

```
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMaCompTable
   dot1agCfmMaCompMhfCreation
```

ethoam association id-permission

Configure id-permission value for MA Entry.

ethoam association *ma_name* **domain** *md_name* **id-permission {none | chassisid | defer}**

Syntax Definitions

ma_name	Association name for the created Ethernet OAM Association.
md_name	Specifies the domain name used while creating the management domain for which this management association is created.
none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.
defer	The contents of the Sender ID TLV are determined by the corresponding MD object 'dot1agCfmMdIdPermission'.

Defaults

parameter	default
none |chassisid | defer	**defer**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

MA must be created before it is modified.

Examples

```
-> ethoam association MA domain MD id-permission defer
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.
show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMaCompTable
   dot1agCfmMaCompMIdPermission
```

ethoam association ccm-interval

Modifies the Continuity Check Message (CCM) transmission interval of an Ethernet OAM Maintenance Association.

ethoam association *ma_name* **domain {***md_name* | *mac_address***} ccm-interval {interval-invalid | interval100ms | interval1s | interval10s | interval1m | interval10m}**

Syntax Definitions

ma_name	Name of the Ethernet OAM Association.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain** command on page 52-5.
interval-invalid	Specifies that no CCMs are sent by a MEP.
interval100ms	Specifies the CCMs are sent every 100 milli seconds.
interval1s	Specifies that CCMs are sent every 1 second.
interval10s	Specifies that CCMs are sent every 10 seconds.
interval1m	Specifies that CCMs are sent every minute.
interval10m	Specifies that CCMs are sent every 10 minutes.

Defaults

parameter	default
interval-invalid | **interval100ms** | **interval1s** | **interval10s** | **interval1m** | **interval10m**	**interval10s**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The *ma_name* should be unique amid all those used by or available to the service provider within a domain.

Examples

```
-> ethoam association MA domain MD ccm-interval interval10s
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMaCompTable
   dot1agCfmMaCompMIdPermission
```

ethoam association endpoint-list

Modifies the MEP list of an Ethernet OAM Maintenance Association.

ethoam association *ma_name* **domain {***md_name* | *mac_add***} endpoint-list** *mep_id***[**-*mep_id2***]**

no ethoam association *ma_name* **domain {***md_name* | *mac_add***} endpoint-list** *mep_id***[**-*mep_id2***]**

Syntax Definitions

ma_name	Name of the Ethernet OAM Association.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain** command on page 52-5.
mac_add	Specifies the CFM system MAC address.
*mep_id***[**-*mep_id2***]**	Specifies the MEP number. Use a hyphen to specify a range of MEP numbers.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove the MEP list.
- Note that only the MEP that is associated with the MEP list of the MA can be configured locally on the bridge or monitored remotely.
- The *ma_name* should be unique within a domain.

Examples

```
-> ethoam association MA domain MD endpoint-list 100-200
-> no ethoam association MA domain MD endpoint-list 100-200
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
    dot1agCfmMdName
dot1agCfmMaNetTable
    dot1agCfmMaNetName
Dot1agCfmMaMepList
    dot1agCfmMaMepListIdentifier
    dot1agCfmMaMepListRowStatus
```

clear ethoam statistics

Clear statistics for all MEPs or for a particular MEP.

clear ethoam statistics [domain *md_name* **association** *ma_name* **endpoint** *mep_id***]**

Syntax Definitions

ma_name	Association name for the created Ethernet OAM Association.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
mep_id	MEP Identifier. Valid Range is 1-8191.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Statistics are cleared for all MEPs if a specific MEP is not entered with this command.

Examples

```
-> clear ethoam statistics
-> clear ethoam statistics domain MD association MA endpoint 10
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam statistics	Displays the Ethernet OAM of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
   alaCfmMepClearStats
   alaCfmGlobalClearStats
```

ethoam default-domain level

Configure the effective level of all default domain entries with the level value set to **no level**.

ethoam default-domain level *num*

no ethoam default-domain

Syntax Definitions

num	The MD level value. The valid range is 0-7.

Defaults

Default value is 0.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The MD level specified with this command applies to all default domain values that are currently set to **no level**.

Examples

```
-> ethoam default-domain level 1
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.

MIB Objects

```
Dot1agCfmDefaultMdLevel
```

ethoam default-domain mhf

Configure the effective MHF value for all default domain entries with MHF value set to **defer**.

ethoam default-domain mhf {none | default | explicit}

no ethoam default-domain

Syntax Definitions

none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.

Defaults

Default value is none.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ethoam default-domain mhf default
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.

MIB Objects

```
dot1agCfmDefaultMdDefMhfCreation
```

ethoam default-domain id-permission

Configures the effective ID permission value for all default domain entries with the ID permission value set to **defer**.

ethoam default-domain id-permission {none | chassisid}

no ethoam default-domain

Syntax Definitions

none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.

Defaults

Default value is none.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> ethoam default-domain id-permission chassisid
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the default domain configuration.

MIB Objects

```
dot1agCfmDefaultMdDefIdPermission
```

ethoam default-domain primary-vlan

Configures the default domain settings for the specified primary VLAN.

ethoam default-domain primary-vlan {*vlan_id***} [level {no-level | *num*}] [mhf {none | default | explicit | defer}] [id-permission {none | chassisid | defer}]**

no ethoam default-domain

Syntax Definitions

vlan_id	VLAN Identifier.
no-level	MD level is inherited from the default domain level.
num	MD Level. Valid range is 0 to 7.
none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.
defer	MHF defers to the default domain MHF value.
none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype, and Chassis ID TLV are to be present.
defer	ID permission defers to the default domain ID permission value.

Defaults

parameter	default
no-level | *num*	**no-level**
none | **explicit** | **default** | **defer**	**defer**
none | **chassisid** | **defer**	**defer**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

On modification of MHF for any primary VID, Automip is invoked for all VLANs associated with this primary VID.

Examples

```
-> ethoam default-domain primary-vlan 10 id-permission chassid level 3 mhf default.
-> ethoam default-domain primary-vlan 10 id-permission chassid
-> ethoam default-domain primary-vlan 10 level 3
-> ethoam default-domain primary-vlan 10 mhf default
-> ethoam default-domain primary-vlan 10 level 3 mhf default
```

Release History

Release 7.3.1; command was introduced..

Related Commands

show ethoam default-domain Displays the information of all the default MD.

MIB Objects

```
dot1agCfmDefaultMdTable
   dot1agCfmDefaultMdComponentId
   dot1agCfmDefaultMdPrimaryVid
   dot1agCfmDefaultMdLevel
```

ethoam endpoint

Creates a Maintenance End Point (MEP) and virtual MEP.

ethoam endpoint *mep_id* **domain** *md_name* **association** *ma_name* **direction {up | down} {port** *chassis/slot/port* **| virtual | linkagg** *agg_id***} [primary-vlan** *vlan_id***]**

no ethoam endpoint *mep_id* **domain** *md_name* **association** *ma_name*

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
ma_name	Association name for the created Ethernet OAM Association.
up	For UP MEP.
down	For DOWN MEP.
chassis	The chassis identifier.
slot/port	Physical slot and port number on which MEP needs to be created.
virtual	Keyword for creating virtual MEP.
agg_id	Linkagg Identifier on which MEP needs to be created.
vlan_id	VLAN Identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to delete a maintenance endpoint.
- The *mep_id* must be unique amid all those used by or available to the service provider in the specified MA.
- The direction for virtual MEP must always be up.
- For creating a virtual MEP the value of port must be given the keyword “virtual”.

Examples

```
-> ethoam endpoint 10 domain MD association MA direction up port 1/1
-> ethoam endpoint 10 domain MD association MA direction down linkagg 1
-> ethoam endpoint 10 domain MD association MA direction down linkagg 1 vlan 10
-> ethoam endpoint 1 domain md1 association ma1 direction up port virtual primary-
vlan 100
-> no ethoam endpoint 10 domain MD association MA
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1a gCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepIfIndex
   dot1agCfmMepPrimaryVid
```

ethoam endpoint admin-state

Configures the administrative state of MEP.

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **admin-state {enable | disable}**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
mac_address	Specifies the CFM system MAC address.
ma_name	Association name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
enable	Administratively enables MEP.
disable	Administratively disables MEP.

Defaults

The default value is disable.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The *mep_id* specified must already exist in the switch configuration.

Examples

```
-> ethoam endpoint 100 domain MD association MA admin-state enable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIndex
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepAdminStatus
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmTransmitting
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepCcmNotReceived
   dot1agCfmMepCcmStreamError
   dot1agCfmMepCcmStreamOther
   dot1agCfmMepRdiReceived
   dot1agCfmMepLastCcmMaFault
   dot1agCfmMepLastCcmCrossConnFault
   dot1agCfmMepCcmOut
   dot1agCfmMepLbmNextSeqNumber
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepLtmIn
   dot1agCfmMepLtrOut
   dot1agCfmMepDefectsPresent
   dot1agCfmMepDefectsAbsent
   dot1agCfmMepRowStatus
```

ethoam endpoint rfp

Enables or disables the Remote Fault Propagation (RFP) on MEP.

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **rfp {enable | disable}**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
mac_address	Specifies the CFM system MAC address.
ma_name	Association name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
enable	Administratively enables RFP on MEP.
disable	Administratively disables RFP on MEP.

Defaults

The default value of RFP is disable.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The *mep_id* specified must already exist in the switch configuration.
- The domain and association must be created before RFP can be enabled.
- The MEP must be an UP MEP. If down MEP is specified, CLI returns with an error.
- The admin state of the MEP must be enabled in order to report faults.
- RFP cannot be enabled on virtual UP MEP since it is not associated with a physical interface.
- It is recommended that if RFP is enabled on a port, then any other violation feature (Link Monitoring or Link Fault Propagation) should not be configured.
- It is recommended that if RFP is enabled on a port, then automatic recovery is disabled for that port.
- If Link Monitoring is configured on a RFP enabled port, then the wait-to-restore timer must be less than the CCM interval.

Examples

```
-> ethoam endpoint 1 domain md1 association ma1 rfp enable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMDTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmRfpEnabled
```

ethoam endpoint ccm

Configures the MEP to generate Continuity Check Messages (CCM).

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **ccm {enable | disable}**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
mac_address	Specifies the CFM system MAC address.
ma_name	Name of the Ethernet OAM association. Up to 48 (minus the domain name length) characters may be used.
enable	Enables MEP to generate CCMs.
disable	Disables MEP to generate CCMs.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain MD association MA ccm enable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIndex
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepAdminStatus
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmTransmitting
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepCcmNotReceived
   dot1agCfmMepCcmStreamError
   dot1agCfmMepCcmStreamOther
   dot1agCfmMepRdiReceived
   dot1agCfmMepLastCcmMaFault
   dot1agCfmMepLastCcmCrossConnFault
   dot1agCfmMepCcmOut
   dot1agCfmMepLbmNextSeqNumber
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepLtmIn
   dot1agCfmMepLtrOut
   dot1agCfmMepDefectsPresent
   dot1agCfmMepDefectsAbsent
   dot1agCfmMepRowStatus
```

ethoam endpoint priority

Configures the priority values for CCMs and Linktrace Messages (LTMs) transmitted by a MEP.

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **priority** *ccm_ltm_priority*

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
mac_address	Specifies the CFM system MAC address.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
ccm_ltm_priority	Priority value for CCMs and LTMs transmitted by the MEP. The valid range is 0–7.

Defaults

parameter	default
ccm_ltm_priority	7

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain MD association MA priority 6
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIndex
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepAdminStatus
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmTransmitting
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepCcmNotReceived
   dot1agCfmMepCcmStreamError
   dot1agCfmMepCcmStreamOther
   dot1agCfmMepRdiReceived
   dot1agCfmMepLastCcmMaFault
   dot1agCfmMepLastCcmCrossConnFault
   dot1agCfmMepCcmOut
   dot1agCfmMepLbmNextSeqNumber
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepLtmIn
   dot1agCfmMepLtrOut
   dot1agCfmMepDefectsPresent
   dot1agCfmMepDefectsAbsent
   dot1agCfmMepRowStatus
```

ethoam endpoint lowest-priority-defect

Configures the lowest priority fault alarm for the lowest priority defect for a MEP.

ethoam endpoint *mep_id* **domain {***md_name* | *mac_address***} association** *ma_name* **lowest-priority-defect** *lowest_priority_defect*

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
mac_address	Specifies the CFM system MAC address.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
lowest_priority_defect	The lowest priority defect that can generate a Fault alarm. Possible values are **xcon**, **rem-err-xcon**, **no-defect**, **mac-rem-err-xcon**, **err-xcon**, and **all-defect**.

Defaults

parameter	default
lowest_priority_defect	mac-rem-err-xcon

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain esd.ale.com association ale-sales lowest-priority-
defect all-defect
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIndex
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepAdminStatus
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmTransmitting
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepCcmNotReceived
   dot1agCfmMepCcmStreamError
   dot1agCfmMepCcmStreamOther
   dot1agCfmMepRdiReceived
   dot1agCfmMepLastCcmMaFault
   dot1agCfmMepLastCcmCrossConnFault
   dot1agCfmMepCcmOut
   dot1agCfmMepLbmNextSeqNumber
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepLtmIn
   dot1agCfmMepLtrOut
   dot1agCfmMepDefectsPresent
   dot1agCfmMepDefectsAbsent
   dot1agCfmMepRowStatus
```

ethoam linktrace

Enables the maintenance entity to initiate transmitting Link Trace Messages (LTM).

ethoam linktrace {target-macaddress *mac_address* **| target-endpoint** *t_mepid***} source-endpoint** *s_mepid* **domain {***md_name* | *mac_address***} association** *ma_name* **[flag [fdb-mpdb | fdbonly]] [hop-count** *hop_count***]**

Syntax Definitions

mac_address	Target MAC address to be transmitted.
t_mepid	Specifies the MEP for which the Loopback message is targeted.
s_mepid	Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
domain *mac_address*	Specifies the CFM system MAC address.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
fdbonly	Specifies that only the MAC addresses learned in a bridge's active data forwarding table will be used to decide the egress port.
hop_count	Indicates the number of hops remaining in this LTM. Each bridge that handles the LTM decreases the value by 1. This decreased value is returned to the LTM. The valid range is 1–2^32.

Defaults

parameter	default
flag	**fdbonly**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- This command allows an operator to generate a LTM for the specified MEP.
- This command signals the MEP that it should transmit a Linktrace message and detect the presence or lack of the corresponding Linktrace messages.

Examples

```
-> ethoam linktrace target-macaddress 10:aa:ac:12:12:ad source 4 domain MD
association flag fdbonly hop-count 32
Transaction Id: 6943

-> ethoam linktrace target-endpoint 15 source 4 domain MD association
Transaction Id: 6934
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain	Displays the information of a specified Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIdentifier
   dot1agCfmMepTransmitLtmFlags
   dot1agCfmMepTransmitLtmTargetMacAddress
   dot1agCfmMepTransmitLtmTargetMepId
   dot1agCfmMepTransmitLtmTargetlsMepId
   dot1agCfmMepTransmitLtmTtl
   dot1agCfmMepTransmitLtmResult
   dot1agCfmMepTransmitEgressIdentifier
```

ethoam loopback

Initiates the transmission of loopback messages from the specified source MEP to the specified target MEP or MAC address. Also triggers the source MEP to detect the presence or lack of a corresponding loopback reply from the target.

ethoam loopback {target-endpoint *t_mepid* **| target-macaddress** *mac_address***} source-endpoint** *s_mepid* **domain** *md_name* **association** *ma_name* **[number** *num***] [data** *string***] [vlan-priority** *vlan_priority***] [drop-eligible {true | false}]**

Syntax Definitions

t_mepid	Specifies the MEP for which the Loopback message is targeted. The valid range is 1-8191.
mac_address	Target MAC address to be transmitted.
s_mepid	Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
num	Number of loopback messages. The valid range is 1-10.
string	Specifies the amount of data to be included in the Data Type Length Value (TLV), if the Data TLV is selected to be sent. The valid range is 1–255.
vlan_priority	VLAN Priority. The valid range is 0-7.
true	Sets the drop eligibility bit in the VLAN tag to true.
false	Sets the drop eligibility bit in the VLAN tag to false.

Defaults

parameter	default
num	1
vlan_priority	CCM priority
drop-eligible {true | false}	**true**

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Source and target MEP-ID, MD and MA must already exist before loopback is initiated.
- If data TLV is not set, then it is not sent in the loopback message.

Examples

```
-> ethoam loopback target-endpoint 10 source-endpoint 20 domain MD association MA
number 3
Reply from 00:0E:B1:6B:43:89: bytes=64 seq=0 time=100ms
Reply form 00:0E:B1:6B:43:89: bytes=64 seq=0 time=112ms
Request timed out.
----00:E0:B1:6B:43:89 ETH-LB Statistics----
3 packets transmitted, 2 packets received, 33% packet loss
round-trip (ms)  min/avg/max = 100/106/112
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain	Displays the information of a specified Management Domain configured on the bridge.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmMepTransmitLbmDestMacAddress
   dot1agCfmMepTransmitLbmDestMepId
   dot1agCfmMepTransmitLbmDestIsMepId
   dot1agCfmMepTransmitLbmMessages
   dot1agCfmMepTransmitLbmDataTlv
   dot1agCfmMepTransmitLbmVlanPriority
   dot1agCfmMepTransmitLbmVlanDropEnable
   dot1agCfmMepTransmitLbmStatus
```

ethoam fault-alarm-time

Configures the timeout value for the Fault Notification Generation Alarm time that specifies the time interval during which one or more defects should be detected before the fault alarm is issued.

ethoam fault-alarm-time *centiseconds* **endpoint** *mep_id* **domain** *md_name* **association** *ma_name*

no ethoam fault-alarm-time endpoint *mep_id* **domain** *md_name* **association** *ma_name*

Syntax Definitions

centiseconds	The Fault Notification Generation Alarm timeout value, in centi seconds. The valid range is 250–1000.
mep_id	Specifies the MEP of a specific MA. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

Defaults

parameter	default
centiseconds	250

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to restore the Fault Notification Generation Alarm timeout value to the default value.
- The Fault Notification Generation Alarm timeout value is configurable per MEP.

Examples

```
-> ethoam fault-alarm-time 500 endpoint 100 domain esd.ale.com association
ale_sales
-> no ethoam fault-alarm-time endpoint 100 domain esd.ale.com association ale_sales
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepFngAlarmTime
```

ethoam fault-reset-time

Configures the timer value for the Fault Notification Generation Reset time that specifies the time interval during which the fault alarm is re-enabled to process faults. The fault alarm will only be re-enabled if no new faults are received during this time interval.

ethoam fault-reset-time *centiseconds* **endpoint** *mep_id* **domain** *md_name* **association** *ma_name*

no ethoam fault-reset-time endpoint *mep_id* **domain** *ma_name* **association** *ma_name*

Syntax Definitions

centiseconds	The Fault Notification Generation Reset timer value, in centi seconds. The valid range is 250–1000.
mep_id	Specifies the MEP of a specific MA. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

Defaults

parameter	default
centiseconds	1000

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to restore the Fault Notification Generation Reset timeout value to the default value.
- The Fault Notification Generation Reset timer value is configurable per MEP.

Examples

```
-> ethoam fault-reset-time 250 end-point 100 domain esd.ale.com association
ale_sales
-> no ethoam fault-reset-time end-point 100 domain esd.ale.com association
ale_sales
```

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam fault-alarm-time	Configures the timeout value for the Fault Notification Generation Alarm time.
show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepFngResetTime
```

ethoam one-way-delay

Initiates a one-way-delay measurement (1DM) to determine the one-way frame delay (latency) and delay variation (jitter) between two MEPs.

ethoam one-way-delay {target-endpoint *t_mepid* **| target-macaddress** *mac_address***} source-endpoint** *s_mepid* **domain** *md_name* **association** *ma_name* **[vlan- priority** *vlan_priority***]**

Syntax Definitions

t_mepid	Target MEP ID. The valid range is 1-8191.
mac_address	Target MAC address.
s_mepid	Source MEP ID. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
vlan_priority	VLAN Priority. The valid range is 0-7.

Defaults

parameter	default
vlan_priority	7

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Source MEP-ID, MD and MA must be created before initiating 1DM.
- When **target-endpoint** is specified then entry must be present in the RMEP table, no matter if its status is RMEP_OK or RMEP_FAILED, before initiating 1DM. So **target-macaddress** can be used to bypass such a restriction.
- Although the OmniSwitch implementation of Ethernet frame delay measurement (ETH-DM) is compliant with ITU-T Y.1731, delay measurement can be performed for both ITU-T Y.1731 and IEEE 802.1ag MEPs.
- If the 1DM is initiated with a **target-macaddress** and an egress port is found for this MAC address, then the 1DM frames are transmitted from that port. Otherwise, 1DM frames are flooded in the MEP's VLAN.
- One-way delay measurement requires NTP clock synchronization between the sending and receiving MEPs.

Examples

```
-> ethoam one-way-delay target-endpoint 10 source-endpoint 12 domain MD association
MA vlan-priority 4
-> ethoam one-way-dealy target-macaddress 00:e0:b1:6a:52:4c source-endpoint 12
domain MD association MA vlan-priority 4
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam one-way-delay	Displays the one-way-delay and jitter parameters for all entries or for the MAC address of a specific MEP.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
alaCfmMepTable
   alaCfmMepOWDTMacAddress
   alaCfmMepOWDTMepIdentifier
   alaCfmMepOWDTPriority
```

ethoam two-way-delay

Initiate a two-way-delay measurement to determine the round-trip latency and jitter between two MEPs. The initiating MEP sends delay measurement message (DMM) frames to the receiving MEP. The receiving MEP responds with delay measurement reply (DMR) frames.

ethoam two-way-delay {target-endpoint *t_mepid* **| target-macaddress** *mac_address***} source-endpoint** *s_mepid* **domain** *md_name* **association** *ma_name* **[vlan- priority** *vlan_priority***]**

Syntax Definitions

t_mepid	Target MEP ID. The valid range is 1-8191.
mac_address	Target MAC address.
s_mepid	Source MEP ID. The valid range is 1–8191.
md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
vlan_priority	VLAN Priority. The valid range is 0-7.

Defaults

parameter	default
vlan_priority	7

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Source MEP-ID, MD and MA must be created before initiating a two-way delay measurement.
- When **target-endpoint** is specified then entry must be present in the RMEP table, no matter if the status is RMEP_OK or RMEP_FAILED, before initiating two-way-delay. So **target-macaddress** can be used to bypass such a restriction.
- The CLI console will pause until all DMRs are received or maximum of 3 seconds to ensure that all the DMRs have been returned. If the operation fails, then the appropriate message is displayed. If the operation is successful, no message is displayed.
- If the DMM is initiated by UP MEP with a **target-macaddress** and the egress port is found for this MAC address, then DMM frames are transmitted from that port. Otherwise, DMM frames are flooded in the MEP's VLAN.
- Two-way delay measurement does *not* require NTP clock synchronization on the sending and receiving MEPs.

- Although the OmniSwitch implementation of Ethernet frame delay measurement (ETH-DM) is compliant with ITU-T Y.1731, delay measurement can be performed for both ITU-T Y.1731 and IEEE 802.1ag MEPs.
- This command initiates an on-demand OAM performance measurement. To set up continuous two-way delay measurement, see the “Service Assurance Agent Commands” chapter for information about how to configure an SAA for continuous two-way frame delay measurement.

Examples

```
-> ethoam two-way-delay target-endpoint 10 source-endpoint 12 domain MD association
MA vlan-priority 4
Reply from 00:0E:B1:6B:43:89 delay=2584us jitter=282us
-> ethoam two-way-delay target-macaddress 00:e0:b1:6a:52:4c source-endpoint 12
domain MD association MA vlan-priority 4
Reply form 00:E0:B1:6A:52:4C: delay=2584us jitter=282us
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam two-way-delay	Displays the two-way-delay delay and jitter parameters for all entries or for the MAC address of a specific MEP.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
alaCfmMepTable
   alaCfmMepTWDTMacAddress
   alaCfmMepTWDTMepIdentifier
   alaCfmMepTWDTPriority
```

clear ethoam

Delete all the one-way-delay or two-way-delay entries.

clear ethoam {one-way-delay-table | two-way-delay-table}

Syntax Definitions

one-way-delay-table	Clears the one-way delay measurement table.
two-way-delay-table	Clears the two-way delay measurement table.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> clear ethoam one-way-delay-table
-> clear ethoam two-way-delay-table
```

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam one-way-delay	Initiates the two one-way-delay messages from a particular MEP to an RMEP.

MIB Objects

```
alaCfmGlobalOWDClear
   alaCfmGlobalTWDClear
```

show ethoam

Displays the information of all the Management Domains (MD) configured on the bridge.

show ethoam

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

This command displays all the MAs for all the MDs.

Examples

```
-> show ethoam
System Configuration
  Ethernet OAM system mac address: 00:D0:95:EC:84:B0,
  Number of Maintenance Domains: 1
    Maintenance Domain: esd.ale.com
        Maintenance Association: ale-sales
```

output definitions

Ethernet OAM system mac address	The MAC address of the Ethernet OAM system.
Number of Maintenance Domains	The number of maintenance domains configured on the bridge.
Maintenance Domain	The name of the maintenance domain.
Maintenance Association	The name of the maintenance association.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam domain	Creates an Ethernet domain with a specific name.

MIB Objects

```
Dot1agCfmMd
   dot1agCfmMdName
Dot1agCfmMa
   dot1agCfmMaName
```

show ethoam domain

Displays the information of a specific Management Domain configured on the bridge.

show ethoam domain *md_name*

Syntax Definitions

md_name	Specifies the management domain name.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD
Total number of MAs configured in this MD = 1
MD Attributes
  MD-Format : string,
  MD-Level : level-3,
  MD-MHFstatus : mhfNone,
  MD-IdPermission : sendIdNone
    Maintenance Association : MA
      MA-Format : string,
      Primary Vlan : 199,
      Associated Vlan-list : none,
      Total Number of Vlans : 1,
      MA-MHFstatus : mhfNone,
      MA-IdPermission : sendIdNone,
      CCM-interval : interval10s,
      MEP-List(MEP-Id) : 10
```

output definitions

MD-level	The level at which the MD was created.
MD-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MD. Options include **none, explicit,** or **default**.
Maintenance Association	The name of the maintenance association.
Vlan	The VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 will be displayed.
MA-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MA. Options include **none, explicit,** or **default**.

output definitions (continued)

CCM-interval	The interval between the CCM transmissions.
MEP-Id	Indicates the Maintenance End Point.

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam	Displays the information of all the Management Domains (MD) configured on the bridge.
ethoam domain	Creates an Ethernet domain with a specific name.

MIB Objects

```
Dot1agCfmMd
   dot1agCfmMdLevel
   dot1agCfmMdMhfCreation
Dot1agCfmMa
   dot1agCfmMaName
   dot1agCfmMaVid
   dot1agCfmMaMhfCreation
   dot1agCfmMaCcmInterval
Dot1agCfmMep
   dot1agCfmMepIdentifier
```

show ethoam domain association

Displays the information of a specific MA in a Management Domain configured on the bridge.

show ethoam domain *md_name* **association** *ma_name*

Syntax Definitions

md_name	Specifies the management domain name.
ma_name	Specifies the name of the Ethernet OAM Association.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD association MA
Total number of MEPs configured in this MA = 1
MA-Format : string,
Primary Vlan : 100,
Associated Vlan-list : none,
Total Number of Vlans : 1,
MA-MHFstatus : mhfDefer,
MA-IdPermission : sendIdDefer,
CCM-interval : interval10s,
MEP-List(MEP-Id) : 1-5,

Legend: MEP-Id: * = Inactive Endpoint

MEP-ID   Admin State Direction   Mac-Address         Port      Primary Vlan
--------+-----------+----------+-------------------+----------+----------------
      1      disable      up    00:E0:B1:A0:78:A3     virtual    100
```

output definitions

Primary Vlan	The VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 will be displayed.
MA-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MA. Options include **none, explicit,** or **default**.
CCM-interval	The interval between the CCM transmissions.
MEP-ID	Indicates the Maintenance End Point.
Admin State	Indicates the administrative state (**up** or **down)** of the MEP.

output definitions (continued)

Direction	The direction of the MEP.
MAC Address	The MAC address of the MEP.
Port	The slot/port number of the Bridge port to which the MEP is attached.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam association	Creates an Ethernet OAM Maintenance Association in the specified domain.

MIB Objects

```
Dot1agCfmMa
   dot1agCfmMaVid
   dot1agCfmMaMhfCreation
   dot1agCfmMaCcmInterval
Dot1agCfmMep
   dot1agCfmMepIdentifier
   dot1agCfmMepActive
   dot1agCfmMepDirection
   dot1agCfmMepIfIndex
   dot1agCfmMepMacAddress
```

show ethoam domain association end-point

Displays the information of a specific MEP in a Management Domain configured on the bridge.

show ethoam domain *md_name* **association** *ma_name* **end-point** *mep_id*

Syntax Definitions

md_name	Specifies the management domain name.
ma_name	Specifies the name of the Ethernet OAM Association.
mep_id	Specifies the MEP of a specific MA. The valid range is 1–8191.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD association MA endpoint 10
Admin State : disable,
Direction : up,
Slot/Port: virtual,
MacAddress: 00:E0:B1:A0:78:A3,
Fault Notification : FNG_RESET,
CCM Enabled : disabled,
RFP Status : enabled,
CCM Linktrace Priority : 7,
CCM Not Received : false,
CCM Error defect : false,
CCM Xcon defect : false,
MEP RDI defect : false,
MEP Last CCM Fault : not specified,
MEP Xcon Last CCM Fault : not specified,
MEP Error Mac Status : false,
MEP Lbm NextSeqNumber : 0,
MEP Ltm NextSeqNumber : 32157,
Fault Alarm Time : 250,
Fault Reset Time : 1000,
Lowest PrDefect Allowed : DEF_MAC_REM_ERR_XCON,
Highest PrDefect Present : DEF_NONE
```

output definitions

Admin State	Indicates the administrative state **(up** or **down**) of the MEP.
Direction	The direction of the MEP.

output definitions (continued)

Slot/Port	The slot/port number of the Bridge port to which the MEP is attached. If the value is virtual, it indicates a virtual port.
MAC Address	The MAC address of the MEP.
Fault Notification	Indicates the current state of the MEP Fault Notification Generator State Machine, which can be **FNG_RESET**, **FNG_DEFECT**, **FNG_REPORT_DEFECT**, **FNG_DEFECT_REPORTED**, or **FNG_DEFECT_CLEARING**.
RFP Status	Indicates the status of the RFP.
CCM Enabled	Indicates whether the MEP generates CCMs (**enabled**) or not (**disabled**).
CCM Linktrace Priority	Indicates the priority value for CCMs and LTMs transmitted by the MEP.
CCM Not Received	Indicates if CCMs are not being received (**true**) or received (**false**) from at least one of the configured remote MEPs.
CCM Error defect	Indicates if a stream of erroneous CCMs is being received (**true**) or not (**false**) from a MEP in this MA.
CCM Xcon defect	Indicates if a stream of CCMs is being received (**true**) or not (**false**) from a MEP that belongs to another MA.
MEP RDI Received	Indicates that any other MEP in this MA is transmitting the RDI bit. Options include **true** or **false**.
MEP Last CCM Fault	The last-received CCM that triggered a MA fault.
MEP Xcon Last CCM Fault	The last-received CCM that triggered a cross-connect fault.
MEP Error Mac Status	Indicates a port status TLV. Options include **true** or **false**.
MEP Lbm NextSeqNumber	The next Transaction Identifier or Sequence Number to be sent in an LBM.
MEP Ltm NextSeqNumber	The next Transaction Identifier or Sequence Number to be sent in an LTM.
Fault Alarm Time	The time interval during which one or more defects should be detected before the fault alarm is issued
Fault Reset Time	The time interval during which the fault alarm is re-enabled to process faults
Lowest PrDefect Allowed	The lowest priority defect that allowed to generate fault alarm.
Highest PrDefect Present	The highest priority defect since the MEPs Fault Notification Generator in reset state.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam endpoint	Creates an Ethernet OAM Maintenance End Point in the specified MA.
ethoam endpoint admin-state	Configures the administrative state of MEP.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepActive
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepSomeRMepCcmDefect
   dot1agCfmMepErrorCcmDefect
   dot1agCfmMepXconCcmDefect
   dot1agCfmMepSomeRdiDefect
   dot1agCfmMepErrorCcmLastFailure
   dot1agCfmMepXconCcmLastFailure
   dot1agCfmMepErrMacStatus
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepFngAlarmTime
   dot1agCfmMepFngAlarmTime
   dot1agCfmMepLowPrDef
   dot1agCfmMepHighestPrDefect
```

show ethoam default-domain configuration

Displays the level, MHF, and ID permission values for the default domain.

show ethoam default-domain configuration

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam default-domain configuration
Level : 3,
MHF-Creation : mhfdefault,
ID-Permission : sendIdnone
```

output definitions

Level	The level assigned to the default domain. Configured through the **ethoam default-domain level** command.
MHF-creation	Indicates the MHF value for a VLAN that is part of the default MD Options include **none**, **explicit**, or **default**. Configured through the **ethoam default-domain mhf** command.
ID-Permission	The ID permision of the default domain. Configured through the **ethoam default-domain id-permission** command.

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam default-domain	Displays the primary VLAN configuration for the default domain.

MIB Objects

```
dot1agCfmMaDefaultMdDefLevel
   dot1agCfmMaDefaultMdDefMhfCreation
   dot1agCfmMaDefaultMdDefIdPermission
```

show ethoam default-domain

Displays all the default MD information for all the primary VLANs or for a specific primary VLAN.

show ethoam default-domain [primary-vlan *vlan_id***]**

Syntax Definitions

vlan_id	The primary VLAN ID.

Defaults

By default, the default MD information for all primary VLANs is displayed.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

Use the *vlan_id* parameter with this command to view information about the default MD for a specific primary VLAN.

Examples

```
-> show ethoam default-domain

Primary-Vlan   Mhf-creation    Level      Id-Permission Status
--------------+-------------+-----------+--------------+--------
      1        mhfDefer       no-level    sendIdDefer    true
      10       mhfDefault         3       sendIdNone     true

-> show ethoam default-domain primary-vlan 10
Primary-Vlan   Mhf-creation    Level      Id-Permission  Status
--------------+-------------+-----------+--------------+--------
      10        mhfDefault        3       sendIdNone     true
```

output definitions

Primary Vlan	The primary VLAN ID of the default MD.
Mhf-creation	The primary VLAN ID MHF value (**none**, **explicit**, or **default**).
Level	The primary VLAN level (**no-level**, **0–7**).
Id-Permission	The primary VLAN ID permission (**none**, **chassid**, or **defer**).

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam default-domain primary-vlan	Modifies the default domain for the specified primary VLAN.

MIB Objects

```
Dot1agCfmDefaultMdLevel
   dot1agCfmDefaultMdLevelVid
   dot1agCfmDefaultMdLevelMhfCreation
   dot1agCfmDefaultMdLevelLevel
```

show ethoam remote-endpoint domain

Displays the information of all remote MEPs learned as a part of the CCM message exchange.

show ethoam remote-endpoint domain *md_name* **association** *ma_name* **end-point** *s_mepid* **[remote-mep** *r_mepid***]**

Syntax Definitions

md_name	Specifies the domain name.
ma_name	Specifies the name of the Ethernet OAM Association.
s_mepid	Specifies the MEP of a specific MA. The valid range is 1–8191.
r_mepid	The remote MEP. The valid range is 1–8191.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam remote-endpoint domain MD association MA endpoint 10
Legends: PortStatusTlv: 1 = psBlocked, 2 = psUp, 0 = psNoTlv
         InterfaceStatusTlv: 1 = ifUp, 2 = ifDown, 4 = ifUnknown, 0=ifNoTlv

RMEP-ID RMEP     OkFailed  Mac Address    port I/f   RDI   Ch-id  Ch-id
        Status    Time                   Tlv  Tlv  value Subtype
------+---------+------+----------------+---+----+-----+--------+------
  20   RMEP_OK   634600 00:E0:B1:6E:41:65  2   1   false LCL-ASND DUT-1
  30   RMEP_OK   334600 00:E0:B1:6E:41:64  2   1   false LCL-ASND DUT-2
```

output definitions

MEP-ID	Indicates the Maintenance End Point.
RMEP Status	The operational state of the remote MEP Remote State machines for this MEP, which can be **RMEP_IDLE**, **RMEP_START**, **RMEP_FAILED**, or **RMEP_OK**.
OkFailed Time	The time (SysUpTime) when the Remote MEP state machine last entered either the **RMEP_FAILED** or **RMEP_OK**.
MacAddress	The MAC address of the remote MEP.
Port Status Tlv	The MAC status TLV last received.
I/f Status Tlv	The interface status TLV last received.

Note: Output shown above is not accurate as it is adjusted to display it in the single row. Following are modified:
P/S Tlv - Port Status Tlv
I/F Tlv - I/F Status Tlv
Ch-id Subtype - Chassis ID Subtype
Ch-id - Chassis ID
LCL-ASND - LOCALLY_ASSIGNED

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain association end-point	Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

dot1agCfmMepDbTable
- dot1agCfmMepDbRMepIdentifier
- dot1agCfmMepDbRMepState
- dot1agCfmMepDbRMepFailedOkTime
- dot1agCfmMepDbRdi
- dot1agCfmMepDbPortStatusTlv
- dot1agCfmMepDbInterfaceStatusTlv
- dot1agCfmMepDbChassisIdSubtype
- dot1agCfmMepDbChassisId

show ethoam cfmstack

Displays the contents of CFM Stack Managed Object, which determines the relationships among MEPs and MIPs on a specific bridge port.

show ethoam cfmstack {port *chassis/slot/port* **| virtual | linkagg** *agg_id***}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	Slot and port number for which the contents of the configured MEP or MIP will be displayed.
virtual	Virtual port.
agg_id	The aggregate ID for which the contents of the configured MEP or MIP will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam cfmstack port 1/3
Up MHF Configured:
  Vlan-id: 100,
  Direction:  up,
  MAC-Address: 00:D0:95:EC:84:B0,
  Maintenance Association: ale-sales,
  Maintenance Domain: esd.ale.com,
  MD-level: 3
Down MHF Configured:
  Vlan-id: 100,
  Direction: down,
  MAC-Address: 00:D0:95:F6:33:DA,
  Maintenance Association: ale-sales,
  Maintenance Domain: esd.ale.com,
  MD-level: 3

-> show ethoam cfmstack port virtual
MEP-Id 32 - Vlan 30:
  Direction: up,
  MAC-Address: 00:E0:B1:A5:F2:34,
  Maintenance Association: MA4,
  Maintenance Domain: MD4,
  MD-level: 4
```

output definitions

Vlan-id	The VLAN ID to which the MEP is attached.
Direction	Indicates the direction (**Inward** or **Outward)** of the Maintenance Point (MP) on the Bridge port.
MAC-Address	The MEP ID configured on this port.
Maintenance Domain	The name of the maintenance domain.
Maintenance Association	The name of the maintenance association.
MD-level	The MD level at which the MD was created.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam endpoint admin-state	Creates an Ethernet OAM Maintenance End Point in the specified MA.

MIB Objects

```
Dot1agCfmMd
   dot1agCfmMdName
Dot1agCfmMa
   dot1agCfmMaName
Dot1agCfmStack
   dot1agCfmStackVlanIdOrNone
   dot1agCfmStackDirection
   dot1agCfmStackMacAddress
   dot1agCfmStackMdLevel
```

show ethoam linktrace-reply

Displays the content of the Linktrace reply (LTR) returned by a previously transmitted LTM. This command displays the LTR based on the transaction identifier or sequence number of the LTM for which the LTR is to be displayed.

show ethoam linktrace-reply domain *md_name* **association** *ma_name* **endpoint** *s_mepid* **tran-id** *num*

Syntax Definitions

md_name	Specifies the domain name.
ma_name	Name of the Ethernet OAM Association.
s_mepid	Specifies the MEP for which the LTR is to be displayed. The valid range is 1-8191.
num	Specifies the Transaction ID or sequence number returned from a previously transmitted LTM.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- "LTM operation successful. Target is reachable." – This message suggests that LTM has reached the target and all the expected LTRs have been received.
- "LTM operation unsuccessful. Target not reachable." – This message suggests that LTM is successfully initiated but the target is not reachable.
- "LTM operation unsuccessful. Target is reachable." – This message suggest that Target is reachable but at least one of the LTR from intermediate hop is not received.
- "LTM operation in progress." – This message suggests that LTM operation is in progress. This message will appear if show CLI is fired before LTM Time-out time.
- "LTM Timed out."- This message suggests that either LTM is not initiated properly or when none of the expected LTRs is received in LTM Time-out duration which is 5 seconds.

Examples

```
-> show ethoam linktrace-reply domain MD association MA endpoint 10 tran-id 1256
LTM operation successful. Target is reachable.
Ttl : 63,
  LTM Forwarded : yes,
  Terminal MEP : no,
  Last Egress Identifier : 00-00:00:D0:95:EA:79:62,
  Next Egress Identifier : 00-00:00:D0:95:EA:9E:BA,
  Relay Action : RLY_FDB,
  Chassis ID Subtype : LOCALLY_ASSIGNED,
```

```
  Chassis ID : DUT-2,
  Ingress Action : ING_OK,
  Ingress Mac : 00:D0:95:EA:9E:D4,
  Ingress Port ID Subtype : LOCALLY_ASSIGNED,
  Ingress Port ID : 1/1,
  Egress Action : EGR_OK,
  Egress Mac : 00:D0:95:EA:9E:D5,
  Egress Port ID Subtype : LOCALLY_ASSIGNED,
  Egress Port ID : 1/2

Ttl : 62,
  LTM Forwarded : no,
  Terminal MEP : yes,
  Last Egress Identifier : 00-00:00:D0:95:EA:9E:BA,
  Next Egress Identifier : 00-00:00:00:00:00:00:00:00,
  Relay Action : RLY_HIT,
  Chassis ID Subtype : LOCALLY_ASSIGNED,
  Chassis ID : DUT-3,
  Ingress Action : ING_OK,
  Ingress Mac : 00:D0:95:EA:AB:D2,
  Ingress Port ID Subtype : LOCALLY_ASSIGNED,
  Ingress Port ID : 1/1,
  Egress Action : EGR_NONE,
  Egress Mac : 00:00:00:00:00:00,
  Egress Port ID Subtype : NONE,
  Egress Port ID : none
```

output definitions

Ttl	Time to live field for the returned LTR.
LTM Forwarded	Indicates whether the LTM was forwarded or not.
Terminal MEP	Indicates whether the MP reported in the reply Ingress/Egress TLV is a MEP.
Last Egress Identifier	Identifies the MEP linktrace initiator that originated, or the responder that forwarded, the LTM to which this LTR is the response.
Next Egress Identifier	Identifies the linktrace responder that transmitted this LTR, and can forward the LTM to the next hop.
Relay Action	Indicates how the dataframe targeted by the LTM would be passed to Egress bridge port. Options include **RLY_HIT**, **RLY_FDB**, or **RLY_MPDB**.
Ingress Action	Indicates how the dataframe targeted by the LTM would be received on the receiving MP. Options include **ING_NONE**, **ING_OK**, **ING_DOWN**, **ING_BLOCKED**, or **ING_VID**.
Ingress Mac	The MAC address returned in the ingress MAC address field.
Egress Action	Indicates how the dataframe targeted by the LTM would be passed through Egress bridge port. Options include **ING_NONE**, **ING_OK**, **ING_DOWN**, **ING_BLOCKED**, or **ING_VID**.
Egress Mac	The MAC address returned in the egress MAC address field.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam linktrace	Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

```
Dot1agCfmLtr
   dot1agCfmLtrTtl
   dot1agCfmLtrForwarded
   dot1agCfmLtrTerminalMep
   dot1agCfmLtrLastEgressIdentifier
   dot1agCfmLtrNextEgressIdentifier
   dot1agCfmLtrRelay
   dot1agCfmLtrIngress
   dot1agCfmLtrIngressMac
   dot1agCfmLtrEgress
   dot1agCfmLtrEgressMac
```

show ethoam linktrace-tran-id

Displays the transaction identifiers returned by previously generated LTMs from a specified MEP.

show ethoam linktrace-tran-id domain {*md_name* | *mac_address***} association** *ma_name* **endpoint** *mep_id*

Syntax Definitions

md_name	Specifies the domain name.
mac_address	Specifies the CFM system MAC address.
ma_name	Name of the Ethernet OAM Association.
mep_id	Specifies the MEP for which the LTR is to be displayed. The valid range is 1-8191.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam linktrace-tran-id domain esd.ale.com association ale-sales endpoint
3
S.No   Transaction Id
-------+----------------------
      1    13357,
      2    13358,
      3    13359,
```

output definitions

S.No	Indicates the sequence number.
Transaction Id	Indicates the Transaction Identifier returned from a previously transmitted LTM.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam linktrace	Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

```
Dot1agCfmLtr
   dot1agCfmLtrSeqNumber
```

show ethoam vlan

Displays the Ethernet OAM statistics of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

show ethoam vlan *vlan_id*

Syntax Definitions

vlan_id	VLAN ID, primary or non-primary VID (e.g. ‘10’).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam vlan 10
Primary Vlan : 10,
Associated Vlan-list : 15-20 25 50-80

-> show ethoam vlan 15
Primary Vlan : 10,
Associated Vlan-list : 15-20 25 50-80
```

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam endpoint	Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

MIB Objects

```
dot1agCfmMaVlanTable
    dot1agCfmVlanVid
    dot1agCfmVlanPrimaryVid
```

show ethoam statistics

Displays the Ethernet OAM of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

show ethoam statistics domain {*md_name* | *mac_address***} [association** *ma_name***] [end-point** *mep_id***]**

Syntax Definitions

md_name	Specifies the domain name.
mac_address	Specifies the CFM system MAC address.
ma_name	Specifies the name of Ethernet OAM Association.
mep_id	Specifies a MEP for a specific MA.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam statistics domain MD
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected   MA
        Out    Error    In   of order  Out     MSDU    LTR In
------+------+-------+------+--------+------+--------+----------+---------
     3    105       0      0        0      0        0          0  MA

-> show ethoam statistics domain MD association MA
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected
        Out    Error    In   of order  Out     MSDU    LTR In
------+------+-------+------+--------+------+--------+----------
     3    105       0      0        0      0        0          0

-> show ethoam statistics domain MD association MA endpoint 3
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected
        Out    Error    In   of order  Out     MSDU    LTR In
------+------+-------+------+--------+------+--------+----------
     3    105       0      0        0      0        0          0
```

output definitions

MEP-Id	The MEP ID configured in the specified MA.
CCM Out	The total number of CCMs transmitted.
CCM Seq Error	The total number of out-of-sequence CCMs received from all remote MEPs.

output definitions

LBR In	The total number of valid, in-order LBRs received.
LBR Out of order	The total number of valid, out-of-order LBRs received.
LBR Out	The total number of LBRs transmitted.
LBR Bad MSDU	The total number of LBRs received whose mac_service_data_unit did not match.
Unexpected LTR In	The total number of unexpected LTRs received.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam endpoint	Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

MIB Objects

```
Dot1agCfmMep
   dot1agCfmMepIdentifier
   dot1agCfmMepCcmOut
   dot1agCfmMepRCcmSequenceErrors
   dot1agCfmMepLbrIn
   dot1agCfmMepLbrInOutOfOrder
   dot1agCfmMepLbrOut
   dot1agCfmMepLbrBadMsdu
   dot1agCfmMepUnexpLtrIn
```

show ethoam config-error

Displays the configuration error for a specified VLAN and port or linkagg.

show ethoam config-error [vlan *vlan_id***] [{port** *chassis/slot/port* **| linkagg** *agg_id***}]**

Syntax Definitions

vlan_id	VLAN Identifier.
chassis	The chassis identifier.
slot/port	Physical slot and port number.
agg_id	Logical link aggregate ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show ethoam config-error
Vlan    Port   Error-type
------+------+------------
10       1/2    CFMleak
10       1/10   CFMleak
30       1/2    CFMleak

-> show ethoam config-error vlan 10
vlan    port   error-type
------+------+------------
10       1/2    CFMleak
10       1/10   CFMleak

-> show ethoam config-error port 1/2
vlan    port   error-type
------+------+------------
10       1/2    CFMleak
30       1/2    CFMleak

-> show ethoam config-error vlan 10 port 1/2
vlan    port   error-type
------+------+------------
10       1/2    CFMleak
```

output definitions

vlan	VLAN identifier number.
port	Physical slot and port number.
error-type	Type of an error.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam linktrace	Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

```
dot1agCfmConfigErrorListTable
   dot1agCfmConfigErrorListVid
   dot1agCfmConfigErrorListIfIndex
   dot1agCfmConfigErrorListErrorType
```

show ethoam one-way-delay

Displays the one-way ETH-DM delay (latency) and jitter parameters either for all entries or for a specified MAC address for a particular source MEP-ID.

show ethoam one-way-delay domain *md_name* **association** *ma_name* **endpoint** *s_mepid* **[mac-address** *mac_address***]**

Syntax Definitions

md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
s_mepid	Source MEP ID. The valid range is 1–8191.
mac_address	MAC Address of the remote MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Dash (‘-‘) in the output in Jitter column signifies that the value can not be calculated as the previous delay value is unknown. This will happen only when 1DM is received for the first time.
- Maximum entries that Delay Result table can store are 1024. After that, the oldest entry is deleted from the table whenever a new entry is required.

Examples

```
-> show ethoam one-way-delay domain MD association MA endpoint 10
Legend: Jitter: - = undefined value

Remote Mac address            Delay (us)  Jitter (us)
--------------------------+-------------+--------------------------------
00:d0:95:ef:44:44              2369          1258
00:d0:95:ef:66:88              5896           282
00:d0:95:ef:88:88              2584           -
00:d0:95:ef:66:55              2698          4782

-> show ethoam one-way-delay domain MD association MA endpoint 10 mac-address
00:d0:95:ef:44:44
Legend: Jitter: - = undefined value

Remote Mac address       Delay (us)   Jitter (us)
-------------------+-------------+-------------------
00:d0:95:ef:44:44        2369           1258
```

output definitions

Remote Mac address	Remote MAC address.
Delay	Physical slot and port number.
eJitter	Type of an error.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam one-way-delay	Initiates one-way-delay messages from a particular MEP to an RMEP.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
alaDot1agCfmMepDelayRsltTable
   alaDot1agCfmMepDelayRMepMacAddress
   alaCfmMepDelayTestType
   alaCfmMepDelayTestDelay
   alaCfmMepDelayVariation
```

show ethoam two-way-delay

Displays the two-way ETH-DM delay and jitter parameters for a specific remote MAC-Address or for all the MAC-Addresses for which two-way-delay was initiated for a particular source MEP-ID.

show ethoam two-way-delay domain *md_name* **association** *ma_name* **endpoint** *s_mepid* **[mac-address** *mac_address***]**

Syntax Definitions

md_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
ma_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
s_mepid	Source MEP ID. The valid range is 1–8191.
mac_address	MAC Address of the remote MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- If ‘0’ appears in the output in RMEP-ID column signifies that the DMM was initiated with target-macaddress. As multiple RMEPs can have same mac-address.
- If a dash (‘-‘) appears in the output in Jitter column signifies that the value can not be calculated as the previous delay value is unknown, i.e. if only one reply for DMM (DMR) is received and this was the first time DMM was initiated from the MEP, then jitter will not be calculated.
- Maximum entries that Delay Result table can store are 1024. After that, the DMM request shall be rejected if a new entry needs to be created for the MEP. If entry for the MEP already exists in the table, that entry shall be updated with the new one.

Examples

```
-> show ethoam two-way-delay domain MD association MA endpoint 10 mac-address
00:d0:95:ef:44:44
Legend: Jitter: - = undefined value
      : RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID   Delay (us)     Jitter (us)
------------------+--------+-------------+-------------
 00:d0:95:ef:44:44   12         2369          1258

-> show ethoam two-way-delay domain MD association MA endpoint 10 remote-mep 0
Legend: Jitter: - = undefined value
      : RMEP-ID: 0 = two-way-delay was initiated with target mac-address
```

```
Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
------------------+--------+-------------+-----------
 00:d0:95:ef:66:88    0         5896   282
 00:d0:95:ef:88:88    0         2584   1856

-> show ethoam two-way-delay domain MD association MA endpoint 10 remote-mep 15
Legend: Jitter: - = undefined value
      : RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
------------------+--------+-------------+-----------
 00:d0:95:ef:66:55   15         2736     -

-> show ethoam two-way-delay domain MD association MA endpoint 10
Legend: Jitter: - = undefined value
      : RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
------------------+--------+-------------+-----------
 00:d0:95:ef:44:44   12         2369  1258
 00:d0:95:ef:66:88    0         5896   282
 00:d0:95:ef:88:88    0         2584   1856
 00:d0:95:ef:66:55   15         2736     -
```

output definitions

Remote Mac address	Remote MAC address.
RMEP-ID	Value of RMEP-ID
Delay	Physical slot and port number.
Jitter	Type of an error.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam two-way-delay	Initiate two-way-delay messages from a particular MEP to an RMEP using target-endpoint or target-MAC address.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
alaDot1agCfmMepDelayRsltTable
   alaCfmMepDelayRMepMacAddress
   alaCfmMepDelayTestType
   alaCfmMepDelayTestDelay
   alaDot1agCfmMepDelayVariation
```

53 LINK OAM Commands

Ethernet in the First Mile (EFM), also known as LINK OAM, is a collection of protocols specified in IEEE 802.3ah, defining Ethernet in the access networks that connects subscribers to their immediate service provider. EFM, EFM-OAM and LINKOAM refers to IEEE 802.3ah standard.

LINK OAM (operation, administration, and maintenance) is a tool which monitors Layer-2 link status on the network by sending OAM protocol data units (OAMPDUs) between the network devices. OAMPDUs contain control and status information used to monitor, test and troubleshoot OAM-enabled links. By enabling LINK OAM on switch ports, network administrators can monitor the link-related issues on the first mile. LINK OAM provides network administrators the ability to monitor link performance, remote fault detection and remote loopback control.

Note. EFM (LINK OAM) does not include functions such as station management, bandwidth allocation or provisioning functions.

MIB information for the EFM (LINK OAM) commands is as

Filename: alcatel-ind1-dot3-oam-mib.mib
Module: ALCATEL-IND1-DOT3-OAM-MIB

Filename: dot3-oam-mib.mib
Module: DOT3-OAM-MIB

A summary of the available commands is listed here:

Global Configuration Commands	**efm-oam admin-state** **efm-oam multiple-pdu-count** **efm-oam errored-frame-seconds-summary** **efm-oam errored-frame-period** **efm-oam errored-frame**
Port Status Commands	**efm-oam port admin-state** **efm-oam port mode** **efm-oam port propagate-events**
Port Event Notification Commands	**efm-oam errored-frame** **efm-oam errored-frame-period** **efm-oam errored-frame-seconds-summary**
Timer Interval Commands	**efm-oam port keepalive-interval** **efm-oam port hello-interval**

Remote Loopback Commands	**efm-oam port remote-loopback** **efm-oam port remote-loopback start** **efm-oam port l1-ping**
Show Commands	**show efm-oam port** **show efm-oam port detail** **show efm-oam port remote detail** **show efm-oam port history** **show efm-oam port l1-ping detail** **show efm-oam port statistics** **show efm-oam configuration**
Clear Commands	**clear efm-oam statistics** **clear efm-oam log-history**

efm-oam admin-state

Enables or disables the LINK OAM protocol on the switch.

efm-oam admin-state {enable | disable}

Syntax Definitions

enable	Enables the LINK OAM protocol.
disable	Disables the LINK OAM protocol.

Defaults

By default, the LINK OAM protocol is disabled for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- LINK OAM must be enabled globally for the OAM to be functional on all the ports.
- When LINK OAM is disabled globally, all dynamically learned information on the port, including peer information, is deleted. However, the LINK OAM configuration for the port is retained.

Examples

```
-> efm-oam admin-state enable
-> efm-oam admin-state disable
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam port admin-state	Enables or disables LINK OAM protocol on the specified port or on a range of ports.
efm-oam port mode	Configures the LINK OAM mode on the port or on the range of ports to active or passive.
show efm-oam configuration	Displays the global LINK OAM configuration.

MIB Objects

```
alaDot3OamStatus
```

efm-oam port admin-state

Enables or disables LINK OAM protocol on the specified port or on a range of ports.

efm-oam port *chassis/slot/port* **[**-*port2***] admin-state {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number of the module and the physical port number on that module.
-port2	Specifies the last port in the range of ports.
enable	Enables LINK OAM protocol on the specified port.
disable	Disables LINK OAM protocol on the specified port.

Defaults

By default, the LINK OAM protocol is disabled on all ports for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- LINK OAM must be enabled globally for the OAM to be functional on all the ports.
- If LINK OAM is disabled for the port or globally disabled for the switch, any OAMPDUs received are discarded.
- When LINK OAM is disabled for the port, all dynamically learned information on the port, including peer information, is deleted. However, the LINK OAM configuration for the port is retained.
- LINK OAM is not supported on the mirroring ports.
- In link aggregates, LINK OAM is supported on an individual aggregable port only.

Examples

```
-> efm-oam port 1/1/1 admin-state enable
-> efm-oam port 1/1/1 admin-state disable
-> efm-oam port 2/1/1-10 admin-state enable
-> efm-oam port 2/1/1-4 admin-state disable
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam port mode	Configure a LINK OAM mode on the port or on the range of ports to active or passive.
show efm-oam configuration	Displays the global LINK OAM configuration.
show efm-oam port	Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.
show efm-oam port detail	Displays the configuration and other related parameters for a port.

MIB Objects

```
dot3OamTable
   dot3OamAdminState
```

efm-oam port mode

Configures the LINK OAM mode on the port or on the range of ports to active or passive.

efm-oam port *chassis/slot/port***[**-*port2***] mode {active | passive}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-port2	Specifies the last port in the range of ports.
active	Configures the LINK OAM mode to active.
passive	Configures the LINK OAM mode to passive.

Defaults

By default, LINK OAM mode is set to active on all ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- LINK OAM discovery process is never initiated from a port when it is in passive mode. At least one of the two peer ports should be in active mode.
- An active port will respond to Loopback-control OAMPDUs only if the peer EFM-OAM client is also in active mode.

Examples

```
-> efm-oam port 1/1/1 mode active
-> efm-oam port 1/1/1 mode passive
-> efm-oam port 2/1/1-10 mode active
-> efm-oam port 2/1/1-4 mode passive
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam port admin-state	Enables or disables LINK OAM protocol on the specified port or on a range of ports.
show efm-oam port	Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.
show efm-oam configuration	Displays the global LINK OAM configuration.

MIB Objects

```
dot3OamTable
   dot3OamMode
```

efm-oam port keepalive-interval

Configures the timeout interval for the dynamically learned neighboring devices on a port or on a range of ports. Keepalive-interval is the maximum time period for which a LINK OAM port shall wait for a hello message from its peer before resetting a discovery session.

efm-oam port *chassis/slot/port***[***-port2***] keepalive-interval** *seconds*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-port2	Specifies the last port in the range of ports.
seconds	Specifies the keep-alive interval value in seconds. The range for this interval is 5 to 120 seconds.

Defaults

By default, the keep-alive interval value is 5 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- Even if unsupported OAMPDU is received on the port, keep-alive timer is reset on the port.
- To set the timer to its default value, set 5 seconds as the keepalive-interval.

Examples

```
-> efm-oam port 1/1/1 keepalive-interval 10
-> efm-oam port 2/1/1-10 keepalive-interval 10
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam port hello-interval	Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of a LINK OAM enabled port.
show efm-oam port detail	Displays the configuration and other related parameters for a port.

MIB Objects

```
alaDot3OamTable
   alaDot3OamKeepAliveInterval
```

efm-oam port hello-interval

Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of an LINK OAM enabled port.

efm-oam port *chassis/slot/port***[**-*port2***] hello-interval** *seconds*

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-*port2*	Specifies the last port in the range of ports.
seconds	Specifies the time interval (in seconds) this port waits before sending out the next hello packet.The range for this timer is 1 to 60 seconds.

Defaults

By default, the hello-interval value is set to 1 second.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- Use the hello-interval value of 1 second to reset the timer to its default value.
- On a given port, hello interval time period should not be more than half of keep alive timer on the peer port.

Examples

```
-> efm-oam port 1/1/1 hello-interval 5
-> efm-oam port 2/1/1-10 hello-interval 10
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam port hello-interval	Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of a LINK OAM enabled port.
efm-oam port keepalive-interval	Configures the timeout interval for the dynamically learned neighboring devices on a port or on a range of ports. Keepalive-interval is the maximum time period for which a LINK OAM port shall wait for a hello message from its peer before resetting a discovery session.
show efm-oam port detail	Displays the configuration and other related parameters for a port.

MIB Objects

```
alaDot3OamTable
   alaDot3OamHelloInterval
```

efm-oam port remote-loopback

Specifies whether loopback requests from peers are processed or ignored on the specified port.

efm-oam port *chassis/slot/port***[**-*port2***] remote-loopback {process | ignore}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-port2	Specifies the last port in the range of ports.
process	Processes incoming loopback request from peer LINK OAM port.
ignore	Ignore (discard) incoming loopback requests.

Defaults

By default, the incoming loopback requests are ignored.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- When the remote-loopback is in **process** mode, the session started by peer LINK OAM client will be processed by local LINK OAM port. As a result, remote port will be in remote-loopback state and the local port will be local-loopback state.
- When the remote-loopback is in **ignore** mode, the session started by peer LINK OAM will not be processed by the local port.

Examples

```
-> efm-oam port 1/1/1 remote-loopback process
-> efm-oam port 1/1/1 remote-loopback ignore
-> efm-oam port 2/1/1-10 remote-loopback process
-> efm-oam port 2/1/1-4 remote-loopback ignore
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam port remote-loopback start	Initiates the loopback control PDU towards the peer port to start or stop the loopback session on the specified port.
show efm-oam port detail	Displays the LINK OAM configuration and other related parameters for a port.
show efm-oam port remote detail	Displays the configuration and details of the related parameters of the remote port.

MIB Objects

```
dot3OamLoopbackTable
   dot3OamLoopbackIgnoreRx
```

efm-oam port remote-loopback start

Initiates the loopback control PDU towards the peer port to start or stop the loopback session on the specified port.

efm-oam port *chassis/slot/port* **remote-loopback {start | stop}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
start	Specifies whether to start the loopback request.
stop	Specifies whether to stop the loopback request.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- Before issuing this command, the LINK OAM port has to be in active mode and discovery of peer ports has to be completed.
- When loopback is started from a port towards a peer port which is configured to ignore the loopback request, the loopback response timer will timeout and no error is displayed. In such case, verify the loopback-state of two ports by using the command **show efm-oam port remote detail**.
- The maximum number of simultaneous loopback sessions supported per network interface is 2. If a third loopback is started through CLI, an error will be displayed at the CLI prompt.

Examples

```
-> efm-oam port 1/1/1 remote-loopback start
-> efm-oam port 1/1/1 remote-loopback stop
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam port remote-loopback	Specifies an action that should perform when a loopback request is received from the peer on a port or on a range of ports.
show efm-oam port remote detail	Displays the configuration and details of the related parameters of the remote port.
show efm-oam configuration	Displays the global LINK OAM configuration.

MIB Objects

```
dot3OamLoopbackTable
   dot3OamLoopbackStatus
```

efm-oam port propagate-events

Configures whether or not the specified port or range of ports will propagate local event notifications to the remote peer.

efm-oam port *chassis/slot/port***[**-*port2***] propagate-events {critical-event | dying-gasp} {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-*port2*	Specifies the last port in the range of ports.
critical-event	Configures the notification status for critical events.
dying-gasp	Configures the notification status for dying gasp events.
enable	Enables the notification of critical-event or dying-gasp events to the peer.
disable	Disables the notification of critical-event or dying-gasp events to the peer.

Defaults

By default, the notification status for both critical-event and dying-gasp events is set to enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- When the system is set for critical event or a dying-gasp event, the local OAM entity indicates the event through the OAMPDU flags to its peer OAM entity.
- In case of port admin down, the OAM IFU-PDU with dying-gasp bit set will be sent to peer as soon as a failure is detected and transmission will continue till the specific port actually goes down.
- In case of takeover or reload of the switch, the OAM IFU-PDU with dying-gasp bit set will be sent to peer as soon as a failure is detected and transmission will continue till the specific device actually goes down.
- The information PDUs with dying gasp bit set is transmitted towards peer as soon as link-down is detected at NI. However, if there is a link flap (i.e link comes again) before the expiry of link-flap timer, then normal information PDU transmission with dying-gasp bit reset shall resume. This will cause clearing of alarms or trap on the peer port.

Examples

```
-> efm-oam port 1/1/1 propagate-events critical-event enable
-> efm-oam port 1/1/1 propagate-events critical-event disable
-> efm-oam port 2/1/1-10 propagate-events dying-gasp enable
```

```
-> efm-oam port 2/1-4 propagate-events dying-gasp disable
```

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port remote detail	Displays the configuration and details of the related parameters of the remote port.
show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

MIB Objects

```
dot3OamEventConfigTable
   dot3OamDyingGaspEnable
   dot3OamCriticalEventEnable
```

efm-oam errored-frame-period

Configures the threshold, window frame values and the status for notification when the number of frame-errors exceed the threshold in a given period of time (specified) by window. When the number of frame errors exceeds a threshold within a given window defined by a number of frames (for example, 10 frames out of 1000 had errors), an Errored Frame Period event is generated.

efm-oam port *chassis/slot/port***[**-*port2***] errored-frame-period [threshold** *threshold_symbols***] [window** *window_frames***] [notify {enable | disable}]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-port2	The last port number in a range of ports that you want to configure on the same slot.
threshold_symbols	Specifies the frame error threshold number. The range supported is 1 to maximum 4 byte integer value (4294967295).
window_frames	Specifies the number of frames used to define a window within which the frame period errors are measured.
enable	Enables notification of the Errored Frame Period event.
disable	Disables notification of the Errored Frame Period event.

Defaults

parameter	default
threshold_symbols	1 frame error
enable | disable	enable

The default for *window_frames* depends on the port-types. The default, minimum and maximum supported values for various port-types are:

port-type	default value	minimum value	maximum value
100 mbps	200000	20000	12000000
1000 X	2000000	200000	120000000
1000 T	2000000	200000	120000000
10 Gig	20000000	2000000	1200000000

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, 9900

Usage Guidelines

- The command can be issued in any order like window, threshold, and notify. However, at least one option needs to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).

Examples

```
-> efm-oam port 1/1/1 errored-frame-period threshold 1 window 3000000 notify enable
-> efm-oam port 1/1/1 errored-frame-period notify disable
-> efm-oam port 2/1/1-4 errored-frame-period threshold 1 window 3000000 notify
enable
-> efm-oam port 2/1/1-2 errored-frame-period notify disable
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam errored-frame	Configures the threshold, window and notify-status for errored-frame on a port. The frame-period measures the frame-errors, within a specified window of time.
efm-oam errored-frame-seconds-summary	Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port. The Errored Seconds are the time in seconds in which at least one frame error has occurred.
show efm-oam port detail	Displays the Errored Frame Period Event threshold, window, and notification parameter values for a port.

MIB Objects

```
dot3OamEventConfigTable
   dot3OamErrFramePeriodWindow
   dot3OamErrFramePeriodThreshold
   dot3OamErrFramePeriodEvNotifEnable
```

efm-oam errored-frame

Configures an error frame threshold or window on a LINK OAM port and set notification status for errored frame events. When the number of frame errors exceeds a threshold within a given window defined by a period of time (for example, 10 frames in 1 second had errors), an Errored Frame Event is generated.

efm-oam port *chassis/slot/port***[**-*port2***] errored-frame [threshold** *threshold_symbols***] [window** *window_seconds***] [notify {enable | disable}]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-port2	The last port number in a range of ports that you want to configure on the same slot.
threshold_symbols	Specifies the frame error threshold number.
window_seconds	Specifies the window of time, in which the frame errors will be measured. The duration should be in units of 100ms.
enable	Enables notification of the Errored Frame event.
disable	Disables notification of the Errored Frame event.

Defaults

parameter	default
threshold_symbols	1 frame error
window_seconds	1 second (10 dsec)
enable | disable	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- The various options, threshold, window and notify can be issued in any order. However, at least one option has to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).

Examples

```
-> efm-oam port 1/1/1 errored-frame threshold 10 window 32 notify enable
-> efm-oam port 1/1/1 errored-frame notify disable
-> efm-oam port 2/1/1-4 errored-frame threshold 10 window 32 notify enable
-> efm-oam port 2/1/1-2 errored-frame notify disable
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam errored-frame-seconds-summary	Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port.
efm-oam errored-frame-period	Configures the threshold, window and notify-status for errored-frame-period errors on a port. The errored-frame-period measures the frame-errors, within a specified window of frames.
show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

MIB Objects

```
dot3OamEventConfigTable
   dot3OamErrFrameWindow
   dot3OamErrFrameThreshold
   dot3OamErrFrameEvNotifEnable
```

efm-oam errored-frame-seconds-summary

Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port. The Errored Seconds are the time in seconds in which at least one frame error has occurred.

efm-oam port *chassis/slot/port***[**-*port2***] errored-frame-seconds-summary [threshold** *threshold_seconds***] [window** *window_seconds***] [notify {enable | disable}]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-port2	The last port number in a range of ports that you want to configure on the same slot.
threshold_symbols	Specifies the frame error threshold number.
window_seconds	Specifies the window of time in which the frame errors will be measured.
enable	Enables notification of the Errored Frame Seconds Summary event.
disable	Disables notification of the Errored Frame Seconds Summary event.

Defaults

parameter	default
threshold_symbols	1 errored frame second
window_seconds	60 seconds. (600 dsec).
enable | disable	enable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- The various options, threshold, window and notify can be issued in any order. However, at least one option has to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).

Examples

```
-> efm-oam port 1/1/1 errored-frame-seconds-summary threshold 1 window 700 notify
enable
-> efm-oam port 1/1/1 errored-frame-seconds-summary notify disable
-> efm-oam port 2/1/1-4 errored-frame-seconds-summary threshold 1 window 700 notify
enable
-> efm-oam port 2/1/1-2 errored-frame-seconds-summary notify disable
```

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam errored-frame	Configures the threshold, window and notify-status for errored-frame on a port. The frame-period measures the frame-errors, within a specified window of time.
efm-oam errored-frame-period	Configures the threshold, window and notify-status for errored-frame-period errors on a port. The errored-frame-period measures the frame-errors, within a specified window of frames.
show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

MIB Objects

```
dot3OamEventConfigTable
   dot3OamErrFrameSecsSummaryWindow
   dot3OamErrFrameSecsSummaryThreshold
   dot3OamErrFrameSecsEvNotifEnable
```

efm-oam multiple-pdu-count

Configures the value of multiple PDU count. When multiple PDU count is set to a specific number in case of any of the threshold cross events, the same event notification PDU will be transmitted that many times towards the peer.

efm-oam multiple-pdu-count *count*

Syntax Definitions

count	Specifies the number of PDUs that have to be sent in case of event-notification TLVs. The range is 1 to 10 PDUs.

Defaults

By default, the PDU-count value is set to 3.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

N/A

Examples

```
-> efm-oam multiple-pdu-count 5
```

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam configuration	Displays the global LINK OAM configuration.
show efm-oam port remote detail	Displays the configuration and details of the related parameters of the remote port.

MIB Objects

```
alaDot3OamMultiplePduCount
```

efm-oam port l1-ping

Configures the number of frames to be sent by the current LINK OAM port to the remote port's MAC address (l1 ping) and the delay between each consecutive sent frames and to start the ping operation.

efm-oam port *chassis/slot/port* **l1-ping [num-frames** *number***] [delay** *milliseconds***] [start]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	Specifies the slot number for the module and the physical port number on that module.
number	Specifies the number of frames that needs to be sent during ping operation. The allowed range of numbers is between 1 to 20.
milliseconds	Specifies time interval between two consecutive PDUs. The allowed range of delay is between 100 to 1000 milliseconds.
start	Specifies to start the ping operation.

Defaults

parameter	default
number	5 frames
milliseconds	1000 milliseconds

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

- The command is valid only when the LINK OAM is enabled globally, port is in active mode, discovery is done, and the port is in remote loopback mode.
- L1 ping can be started only when the port is in remote loopback mode.

Examples

```
-> efm-oam port 1/1/12 l1-ping num-frames 6 delay 300 start
-> efm-oam port 1/1/20 l1-ping num-frames 12 delay 500 start
-> efm-oam port 1/1/15 l1-ping num-frames 5 delay 100 start
-> efm-oam port 1/1/15 l1-ping num-frames 4 delay 200 start
-> efm-oam port 1/1/5 l1-ping num-frames 100 delay 300 start
```

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port l1-ping detail	Displays the frames lost during a loopback session.
show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

MIB Objects

```
alaDot3OamLoopbackTable
   alaDot3OamPortL1PingFramesConf
   alaDot3OamPortL1PingFramesDelay
   alaDot3OamPortL1PingStatus
   alaDot3OamPortL1PingFramesSent
   alaDot3OamPortL1PingFramesReceived
   alaDot3OamPortL1PingAverageRoundTripDelay
```

show efm-oam configuration

Displays the global LINK OAM configuration.

show efm-oam configuration

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

Use this command to display the global configuration of LINK OAM.

Examples

```
-> show efm-oam configuration
EFM OAM Status                : enabled,
Multiple PDU Count            : 5
```

Output fields are described here:

output definitions

EFM OAM status	The current administrative status of LINK OAM on this switch (**Enabled** or **Disabled**).
Multiple PDU Count	The number of PDUs sent when LINK OAM needs to send multiple Event Notification.

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam admin-state	Enables or disables the LINK OAM protocol on the switch.
show efm-oam port detail	Displays the LINK OAM configuration and other related parameters for a port.

MIB Objects

```
alaDot3OamStatus
   alaDot3OamMultiplePduCount
```

show efm-oam port

Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.

show efm-oam port [*chassis/slot/port1-port2***] [enable | disable] [active | passive]**

Syntax Definitions

chassis	The chassis identifier.
slot/port1	The slot number for the module and the physical port number on that module.
-port2	The last port number in a range of ports that you want to configure on the same slot (e.g. 3/1-4 specifies ports 1,2,3, and 4 on slot 3).
enable	Specifies whether to display the LINK OAM enabled ports.
disable	Specifies whether to display the LINK OAM disabled ports.
active	Specifies whether to display the LINK OAM active ports.
passive	Specifies whether to display the LINK OAM passive ports.

Defaults

By default, displays the LINK OAM status on all ports.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

Use this command to display the state of LINK OAM on the basis of enabled or disabled port and on the basis of active or passive port.

Examples

```
-> show efm-oam port
Port   EFM-OAM Status      Mode  Operational Status  Loopback Status
-------+---------------+---------+------------------+---------------
1/1/1          enabled    active     operational           remoteLoopback
1/1/2         disabled    active     activeSendLocal       noLoopback
1/1/3          enabled   passive     activeSendLocal       noLoopback
1/1/4         disabled    active     activeSendLocal       noLoopback
1/1/5         disabled    active     activeSendLocal       noLoopback
1/1/6         disabled    active     activeSendLocal       noLoopback
1/1/7         disabled    active     activeSendLocal       noLoopback

-> show efm-oam port 1/1-5
Port   EFM-OAM Status      Mode  Operational Status  Loopback Status
-------+---------------+---------+------------------+---------------
1/1/1          enabled    active     operational           remoteLoopback
1/1/2         disabled    active     activeSendLocal       noLoopback
1/1/3          enabled   passive     activeSendLocal       noLoopback
```

```
1/1/4         disabled    active     activeSendLocal       noLoopback
1/1/5         disabled    active     activeSendLocal       noLoopback

-> show efm-oam port 1/1-3 enabled
Port   Mode       Operational Status   Loopback Status
-------+---------------+---------+------------------+----------------
1/1/1   active     operational          remoteLoopback
1/1/3   passive    activeSendLocal      noLoopback

-> show efm-oam port enabled
Port         Mode  Operational Status  Loopback Status
---------+--------+------------------+----------------
1/1/1      active     activeSendLocal   remoteLoopback
1/1/3     passive     activeSendLocal       noLoopback
1/1/7     passive     activeSendLocal       noLoopback

-> show efm-oam port disabled
Port         Mode  Operational Status  Loopback Status
---------+--------+------------------+----------------
1/1/2      active     activeSendLocal       noLoopback
1/1/4     passive     activeSendLocal       noLoopback
1/1/5      active     activeSendLocal       noLoopback

-> show efm-oam port enabled passive
Port   Operational Status  Loopback Status
---------+--------+------------------+----------------
1/1/3   activeSendLocal       noLoopback
1/1/7   activeSendLocal       noLoopback

-> show efm-oam port active
Port   EFM-OAM Status   Operational Status  Loopback Status
------+----------------+--------------------+-------+----------------
1/1/1    enabled         activeSendLocal      remoteLoopback
1/1/2    disabled        activeSendLocal      noLoopback
1/1/3    enabled         activeSendLocal      noLoopback
1/1/4    disabled        activeSendLocal      noLoopback
1/1/5    disabled        activeSendLocal      noLoopback
1/1/6    disabled        activeSendLocal      noLoopback
1/1/7    disabled        activeSendLocal      noLoopback
```

Output fields are described here:

output definitions

Port	Displays the chassis/slot/port number.
EFM-OAM Status	The state of the EFM-OAM. LINK OAM instance can have any of the following status. • **Enabled :** Specifies that the LINK OAM is disabled on the interface. • **Disabled** : Specifies that the LINK OAM is disabled on the interface.

output definitions (continued)

Operational Status	The status of the port in discovering whether the peer has LINK OAM capability or not.It has the following states: • **activeSendLocal**: Specifies that the LINK OAM port is actively trying to discover whether the peer has LINK OAM capability but has not yet made that determination. • **sendLocalAndRemote**: Specifies that the local LINK OAM port has discovered the peer but has not yet accepted or rejected the configuration of the peer. The local device will then decide that the peer device is acceptable or unacceptable and then accept or decline LINK OAM peering. • **sendLocalAndRemoteOk**: Specifies the state when LINK OAM peering is allowed by the local port. • **oamPeeringLocallyRejected**: Specifies the state when the local OAM entity rejects the peer OAM entity. • **oamPeeringRemotelyRejected**: Specifies the state when the remote LINK OAM port rejects the peering. • **operational**: Specifies the state when the local LINK OAM port learns that both the local LINK OAM entity and the remote LINK OAM entity have accepted the peering. • **nonOperHalfDuplex**: Specifies the value nonOperHalfDuplex is returned whenever LINK OAM is enabled. Since LINK OAM functions are not designed to work completely over half-duplex interfaces, the value nonOperHalfDuplex is returned whenever LINK OAM is enabled but the interface is in half-duplex operation. • **linkFault**: Specifies that the link between the host and the peer has detected a fault. • **passiveWait**: Specifies that the LINK OAM ports are in passive mode.
Loopback Status	The state of remote loopback. It can be **initiatingLoopback**, **terminatingLoopback**, **localLoopback**, **remoteLoopback, noLoopback**, or **unknown**.
Mode	The state of LINK OAM mode, **active** or **passive**.

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam multiple-pdu-count	Configures the value of multiple PDU count. When multiple PDU count is set to a specific number in case of any of the threshold cross events, the same event notification PDU will be transmitted that many times towards the peer.

MIB Objects

```
dot3OamTable
   dot3OamAdminState
   dot3OamMode
   dot3OamOperStatus
   dot3OamLoopbackTable
   dot3OamLoopbackStatus
```

show efm-oam port detail

Displays the LINK OAM configuration and other related parameters for a port.

show efm-oam port *chassis/slot/port* **detail**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

Use this command when you want to get LINK OAM configuration details for a specific port.

Examples

```
-> show efm-oam port 1/1/1 detail
OAM Status                   : enable,
Operational Status           : activeSendLocal,
Mode                         : active,
Max OamPDU size              : 1518,
Config Revision              : 0,
Functions Supported          : loopback,event notification,
Loopback Status              : noLoopback,
Loopback Rx Status           : ignore,
Max OamPDUs                  : 10,
KeepAlive Interval(seconds)  : 10,
Hello Interval(seconds)      : 5,
Dying Gasp Notify Status     : enable,
Critical Event Notify Status : enable

    Link Monitoring             Window           Threshold       Notify
                                                  (errors)       Status
------------------+------------+-------------+------------+---------------
errored-frame                   10  dsec          10  frames       enable
errored-frame-period            2000000 frames    10  frames       enable
errored-frame-seconds-summary   600 dsec          1  framesec      enable
```

Output fields are described here:

output definitions

OAM Status	The state of LINK OAM on the port.
Operational Status	The state of the port in discovering whether the peer has LINK OAM capability or not.
Mode	The state of LINK OAM mode on the port, **active** or **passive**.
Max OamPDU size	Displays the maximum OAMPDU that the LINK OAM port can support.
Config Revision	Displays the configuration revision of the LINK OAM port as reflected in the latest OAMPDU sent by the peer port.
Functions Supported	Displays the LINK OAM functions supported by the specified port.
Loopback Status	Displays the loopback status of the specified LINK OAM port.
Loopback Rx Status	The action that should be performed by the LINK OAM port when a loopback request is received from the peer port.
Max OamPDUs	Specifies the maximum OAMPDUs that can be exchanged between two peers.
KeepAlive Interval	Displays the timeout interval of the specified LINK OAM port for the dynamically learned peer port.
Hello Interval	Displays the time interval between two OAMPDUs in seconds.
Dying Gasp Notify Status	The state of notification for dying gasp events, **enable** or **disable**.
Critical Event Notify Status	The state of notification for critical events, **enable** or **disable.**
Link Monitoring	Displays the errors detected on the remote link.
Window	The frame error event window in the received OAMPDU.
Threshold	The number of errored frames in the period required for the event to be generated.
Notify Status	The state of notification for LINK OAM errors on the port, **enable** or **disable**.

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port	Displays the status of LINK OAM on all the ports in the system, along with other relevant information like OAM mode, operational status and loopback status of the port.

MIB Objects

```
dot3OamTable
   dot3OamAdminState
   dot3OamOperStatus
   dot3OamMode
   dot3OamMaxOamPduSize
   dot3OamConfigRevision
   dot3OamFunctionsSupported
alaDot3OamTable
   alaDot3OamKeepAliveInterval
   alaDot3OamHelloInterval
dot3OamLoopbackTable
   dot3OamLoopbackStatus
   dot3OamLoopbackIgnoreRx
dot3OamEventConfigTable
   dot3OamDyingGaspEnable
   dot3OamCriticalEventEnable
   dot3OamErrFramePeriodWindow
   dot3OamErrFramePeriodThreshold
   dot3OamErrFramePeriodEvNotifEnable
   dot3OamErrFrameWindow
   dot3OamErrFrameThreshold
   dot3OamErrFrameEvNotifEnable
   dot3OamErrFrameSecsSummaryWindow
   dot3OamErrFrameSecsSummaryThreshold
   dot3OamErrFrameSecsEvNotifEnable
```

show efm-oam port statistics

Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

show efm-oam port *chassis/slot/port***[**-*port2***] statistics**

show efm-oam port statistics

Syntax Definitions

chassis	The chassis identifier.
slot/port	Specifies the slot number for the module and the physical port number on that module
-port2	The last port number in a range of ports that you want to configure on the same slot.

Defaults

By default, the statistics of all ports are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

Use the **port** parameter to display the statistics of a specific port.

Examples

```
-> show efm-oam port 1/1/1 statistics
Port 1/1/1:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

-> show efm-oam port 1/1-4 statistics
Port 1/1:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
```

```
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/2:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU Tx : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/3:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/4:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0


-> show efm-oam statistics
Port 1/1:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0
```

```
Port 1/2:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0

Port 1/3:
  Information OAMPDU Tx                  : 1035,
  Information OAMPDU Rx                  : 988,
  Unique Event Notification OAMPDU Tx    : 0,
  Unique Event Notification OAMPDU Rx    : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx             : 1,
  Loopback Control OAMPDU Rx             : 0,
  Unsupported OAMPDU Tx                  : 0,
  Unsupported OAMPDU Rx                  : 0,
  Frames Lost due to OAM                 : 0
```

Output fields are described here:

output definitions

Information OAMPDU Tx	The number of OAM PDUx transmitted by the port.
Information OAMPDU Rx	The number of OAM PDUx received by the port.
Unique Event Notification OAMPDU Tx	The number of unique event notification OAM PDUs transmitted by the port.
Unique Event Notification OAMPDU Rx	The number of unique event notification OAM PDUs received by the port.
Duplicate Event Notification OAMPDU TX	The number of duplicate event notification OAM PDUs transmitted by the port.
Duplicate Event Notification OAMPDU Rx	The number of duplicate event notification OAM PDUs received by the port.
Unsupported OAMPDU Tx	The number of unsupported OAM PDUs transmitted by the port.
Unsupported OAMPDU Rx	The number of unsupported OAM PDUs received by the port.
Frames Lost due to OAM	The number of frames discarded by the OAM port.

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port history	Displays the log of events that have occurred on a port. This command can also be used to display specific event logs on a port.

MIB Objects

```
dot3OamStatsTable
   dot3OamInformationTx
   dot3OamInformationRx
   dot3OamUniqueEventNotificationTx
   dot3OamUniqueEventNotificationRx
   dot3OamDuplicateEventNotificationTx
   dot3OamDuplicateEventNotificationRx
   dot3OamLoopbackControlTx
   dot3OamLoopbackControlRx
   dot3OamUnsupportedCodesTx
   dot3OamUnsupportedCodesRx
   dot3OamFramesLostDueToOam
```

show efm-oam port remote detail

Displays the LINK OAM configuration and details of the related parameters of the remote port.

show efm-oam port *chassis/slot/port* **remote detail**

Syntax Definitions

chassis	The chassis identifier.
slot/port	Specifies the slot number for the module and the physical port number on that module.

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

N/A.

Examples

```
-> show efm-oam port 1/1/1 remote detail
Remote MAC address  : 00:30:96:fd:6b:fa,
Remote Vendor (info): 0x15a1
Remote Vendor (oui) : XYZ
Mode                : active,
Max OAMPDU size     : 1518,
Config Revision     : 0,
Functions Supported : loopbackSupportEventSupport
```

Output fields are described here:

output definitions

Remote MAC address	Displays the MAC address of the remote peer.
Remote Vendor (info)	Displays the vendor number in hexadecimal of the remote peer.
Remote Vendor (oui)	Displays the Organizationally Unique Identifier (OUI) number of the remote peer.
Mode	The state of LINK OAM mode on the remote port, **active** or **passive**.
Max OAMPDU size	Displays the maximum OAMPDU size that the remote LINK OAM port can support.
Config Revision	Displays the configuration revision of the remote LINK OAM port.
Functions Supported	Displays the LINK OAM functions supported by the remote port.

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port history	Displays the log of events that have occurred on a port. This command can also be used to display specific event logs on a port.
clear efm-oam statistics	Clears the LINK OAM statistics on a port.

MIB Objects

```
dot3OamPeerTable
   dot3OamPeerMacAddress
   dot3OamPeerVendorOui
   dot3OamPeerVendorInfo
   dot3OamPeerMode
   dot3OamPeerMaxOamPduSize
   dot3OamPeerConfigRevision
   dot3OamPeerFunctionsSupported
```

show efm-oam port history

Displays the log of events that have occurred on a port. Use this command to display specific event logs on a port.

show efm-oam port *chassis/slot/port* **history [log-type { link-fault | errored-frame | errored-frame-period | errored-frame-seconds | dying-gasp | critical}]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	Specifies the slot number for the module and the physical port number on that module.
link-fault	Displays link fault event logs. Specifies the loss of signal is detected by the receiver. This is sent once per second in the Information OAMPDU
errored-frame	Displays errored-frame event log. an errored frame event occurs when the number of detected error frames over a specific interval exceeds the predefined threshold.
errored-frame-period	Displays an errored-frame-period event logs. An errored frame period event occurs if the number of frame errors in specific number of received frames exceeds the predefined threshold.
errored-frame-seconds	Displays errored-frame-seconds event logs. When the number of error frame seconds detected on a port over a detection interval reaches the error threshold, an errored frame seconds event occurs.
dying-gasp	Specifies an unrecoverable condition (e.g., a power failure).
critical	Specifies a crucial event that has occurred on the port.

Defaults

By default, all log types are displayed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

Timestamp will be in following format:

DAY MON Date hh:mm:ss yyyy

Examples

```
-> show efm-oam port 1/1/1 history
Legend: Location: * - Remote, # - Local
LogID   TimeStamp                Log Type          Event
                                                   Total
------+------------------------+-------------+-------+----+
*    1     TUE JAN 06 19:44:51 2009   linkFault       1
#    2     TUE JAN 06 19:45:51 2009   erroredFrame    1
```

```
-> show efm-oam port 1/1/1 history log-type link-fault
Legend: Location: * - Remote, # - Local
LogID   TimeStamp                    Event
                                     Total
-----+---------+---------+------+-----------+
*   1      TUE JAN 06 19:46:51 2009     1
#   2      TUE JAN 06 19:46:51 2009     1
```

Output fields are described here:

output definitions

LogID	Specifies individual events within the event log.
Timestamp	The value of actual time at the time of the logged event.
Log Type	Specifies the type of event log.
Event Total	Specifies the total number of times one or more of these occurrences have resulted in an Event Notification.

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
clear efm-oam log-history	Clears the LINK OAM event logs history on a port.

MIB Objects

```
dot3OamEventLogTable
   dot3OamEventLogIndex
   dot3OamEventLogTimestamp
   dot3OamEventLogOui
   dot3OamEventLogType
   dot3OamEventLogLocation
   dot3OamEventLogWindowHi
   dot3OamEventLogWindowLo
   dot3OamEventLogThresholdHi
   dot3OamEventLogThresholdLo
   dot3OamEventLogValue
   dot3OamEventLogRunningTotal
   dot3OamEventLogEventTotal
```

show efm-oam port l1-ping detail

Displays the frames lost during a loopback session.

show efm-oam port *chassis/slot/port* **l1-ping detail**

Syntax Definitions

chassis	The chassis identifier.
slot/port	Specifies the slot number for the module and the physical port number on that module.

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

The command can also be used even on a port on which LINK OAM is not enabled.

Examples

```
-> show efm-oam port 1/1/1 l1-ping detail
frames configured              = 5,
frames delay(msec)             = 100,
L1 ping status                 = Sucessful,
frames sent                    = 4,
frames received                = 4,
avg delay (msec)               = 5
-> show efm-oam port 1/1/4 l1-ping detail
frames configured              = 5,
frames delay(msec)             = 200,
L1 ping status                 = Successful,
frames sent                    = 4,
frames received                = 2,
avg delay (msec)               = 15
```

Output fields are described here:

output definitions

frames configured	Specifies the number of frames that are sent during l1-ping.
delay configured	Specifies the delay between transmission of two consecutive frames during L1 ping.
L1 ping status	The status of the L1 ping operation. The status can be **Successful**, **Unsuccessful** or **default.**
frames sent	Specifies the frames sent during last L1 ping.

output definitions (continued)

frames received	Specifies the frames received during last L1 ping.
average delay	Specifies the average delay taken by frames during last L1 ping.

Release History

Release 8.5R4; command was introduced.

Related Commands

efm-oam port l1-ping	Configures the number of frames that needs to be sent during L1-ping, the delay between each consecutive sent frames and to start the L1-ping operation.

MIB Objects

```
alaDot3OamLoopbackTable
   alaDot3OamPortL1PingFramesConf
   alaDot3OamPortL1PingFramesDelay
   alaDot3OamPortL1PingStatus
   alaDot3OamPortL1PingFramesSent
   alaDot3OamPortL1PingFramesReceived
   alaDot3OamPortL1PingAverageRoundTripDelay
```

clear efm-oam statistics

Clears the LINK OAM statistics on a port, range of ports or all ports.

clear efm-oam statistics [port *chassis/slot/port***[**-*port2*]]

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-port2	Specifies the last port in the range of ports.

Defaults

By default, the statistics are cleared for all the ports if no port is specified in the command.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

Use the port parameter with this command to clear the statistics for a specific port or range of ports.

Examples

```
-> clear efm-oam statistics
-> clear efm-oam statistics port 1/1/1
-> clear efm-oam statistics port 2/1/1-3
```

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
clear efm-oam log-history	Clears the LINK OAM event logs history on a port.

MIB Objects

```
alaDot3OamGlobalClearStats
   alaDot3OamStatsTable
   alaDot3OamPortClearStats
```

clear efm-oam log-history

Clears the LINK OAM event logs history a port, range of ports or all ports.

clear efm-oam log-history [port *chassis/slot/port***[**-*port2*****]]**

Syntax Definitions

chassis	The chassis identifier.
slot/port	The slot number for the module and the physical port number on that module.
-port2	Specifies the last port in the range of ports.

Defaults

By default, the event logs are cleared for all the ports if no port is specified in the command.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865

Usage Guidelines

Use the port parameter with this command to clear the statistics for a specific port or range of ports.

Examples

```
-> clear efm-oam log-history
-> clear efm-oam log-history port 1/1/1
-> clear efm-oam log-history port 2/1/1-3
```

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port statistics	Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
show efm-oam port history	Displays the log of events that have occurred on a port. Use this command to display specific event logs on a port.

MIB Objects

```
alaDot3OamGlobalClearEventLogs
   alaDot3OamEventLogTable
   alaDot3OamPortClearEventLogs
```

54 CPE Test Head Commands

The Customer Provider Edge (CPE) Test Head traffic generator and analyzer is a Test-OAM (Operation, Administration, and Maintenance) tool used in the Metro Ethernet Network to validate the customer Service Level Agreements (SLA). This functionality allows the operator to validate the Metro Ethernet Network between customer end points, which is critical when provisioning or troubleshooting network services.

This implementation of CPE Test Head supports unidirectional and bidirectional ingress tests. Traffic is generated at the UNI port as if the traffic was generated from a test head connected to the UNI port. This validates the actual customer SLA by subjecting the test traffic to the ingress QoS defined at the UNI port (Ethernet SAP profile or QoS policy rules for priority and bandwidth control) and the egress QoS defined at the egress NNI port and carrier network.

The CPE test is non-disruptive to traffic running on other UNI ports that are associated with the same SAP profile as the test UNI port. All UNI ports, including CPE test ports, are subject to any SAP profile or QoS configuration associated with the port. This is important to consider when analyzing test results.

The feature provides a multi-stream test capability. The CPE multi-test feature is supported on non-metro switches with metro license. The feature supports a stack containing up to eight switches.

Multi-stream test requires a free port. The port must not be used and not have any configuration. When a multi-stream test starts, the port is made out of service. The port is made operational again and the configuration is retained when the test is stopped.

MIB information for the CPE Test Head commands are:

Filename: alcatelIND1testoam.mib
Module: ALCATEL-IND1-TEST-OAM-MIB

A summary of available commands is listed here:

Single-test	**test-oam** **test-oam direction** **test-oam src-endpoint dst-endpoint** **test-oam port** **test-oam vlan test-frame** **test-oam role** **test-oam duration rate packet-size** **test-oam frame** **test-oam l2-saa** **test-oam start stop** **test-oam remote-sys-mac** **test-oam statistics flash-logging** **show test-oam** **show test-oam saa statistics** **clear test-oam statistics**
Multi-test	**test-oam group** **test-oam group tests** **test-oam feeder** **test-oam group src-endpoint dst-endpoint** **test-oam group role** **test-oam group port** **test-oam group direction** **test-oam group duration rate** **test-oam group start stop** **test-oam group remote-sys-mac** **show test-oam group** **show test-oam group statistics** **clear test-oam group statistics**

test-oam

Configures the CPE test name and an optional description. The test name is used to identify and configure a CPE test profile.

test-oam *string* **[descr** *description***]**

no test-oam *string*

Syntax Definitions

string	The name of the CPE test, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test and is also referred to as the test ID.
description	The description to assign to the test name, an alphanumeric string between 1 and 32 characters.

Defaults

parameter	default
description	DEFAULT

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the **no** form of this command to remove the specified CPE test configuration.
- This command creates a new CPE test profile that is identified by the test name. Make sure the name specified does not exist in the switch configuration.
- A maximum of 32 tests can be configured.
- Only one test can be active on the switch at any given time.

Examples

```
-> test-oam Test1
-> test-oam Test2 descr second-test
-> no test-oam Test2
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam	Displays the CPE test configuration and status.
show test-oam statistics	Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigTestDescription
   alaTestOamConfigRowStatus
```

test-oam direction

Configures the CPE test direction.

test-oam *string* **[direction {unidirectional | bidirectional}]**

Syntax Definitions

string	The name of the CPE test, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test and is also referred to as the test ID.
direction	The direction of the CPE test.

Defaults

parameter	default
unidirectional | bidirectional	unidirectional

Platforms Supported

OmniSwitch 6465

Usage Guidelines

This command assigns the direction to the CPE test.

Examples

```
-> test-oam Test1 direction unidirectional
-> test-oam Test1 direction bidirectional
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam	Displays the CPE test configuration and status.
show test-oam statistics	Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigDirection
```

test-oam src-endpoint dst-endpoint

Configures the source and destination endpoints for the specified test.

test-oam *string* **[src-endpoint** *src-string***] [dst-endpoint** *dst-string***]**

Syntax Definitions

string	The name of an existing CPE test. The string can be of length 1to 32 characters.
src-string	This represents the local or transmitting device. The management IP address or DNS host name of the switch that will transmit test traffic. In case of bidirectional test this also identifies the analyzer device. The string can be of length 1to 32 characters.
dst-string	This represents the remote device. The management IP address or DNS host name of the switch that will receive test traffic. This is the switch on which traffic analysis is done. For unidirectional test this represents the analyzer device. For bidirectional test this identifies the device on which the loopback mode must be active. The string can be of length 1to 32 characters.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- The end point can be set as switch hostname or switch management IP address.
- Using the DNS host name of the switch is highly recommended, as this name is unique and is mapped to an IP address configured for the switch.
- This command automatically overwrites the source and destination endpoint values previously configured for the specified CPE test.
- Multicast and broadcast address must not be configured for bidirectional test.

Examples

```
-> test-oam Test1 src-endpoint SW1 dst-endpoint SW2
-> test-oam Test1 src-endpoint SW1
-> test-oam Test1 dst-endpoint SW2
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam port	Configures the port on which the CPE test will run.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigSourceEndpoint
   alaTestOamConfigDestinationEndpoint
```

test-oam port

Configures the port on which the CPE test will run. Use this command on the switch that will generate the test traffic. If the switch is going to receive test traffic, configuring a test port is not necessary.

test-oam *string* **port** *chassis/slot/port*

Syntax Definitions

string	The name of an existing CPE test.
chassis/slot/port	The port on which the CPE test will generate traffic.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- In an Ethernet Service environment, the UNI port is designated as the test port on the generator switch to simulate traffic coming in on the port as if it was sent from a test head device. This will subject the test traffic to the SAP profile.
- Note that the customer traffic is disrupted on ports configured as CPE test ports. Configuring a port that is not in use is recommended. In addition, if the test port is a UNI port associated with an SAP profile, only that UNI port is used for the test. Traffic on other UNI ports associated with the same profile is *not* disrupted by the CPE test.
- All UNI ports, including CPE test ports, are subject to any SAP profile or QoS configuration associated with the port. This must be considered when test results are analyzed.
- This command automatically overwrites the port value previously configured for the specified CPE test.

Examples

```
-> test-oam Test1 port 1/1/2
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam vlan test-frame	Configures the source mac-address, destination mac-address, and the SVLAN for the test-frame used in the test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigPort
```

test-oam vlan test-frame

Configures the SVLAN and the source and destination MAC addresses for the test frame. Use this command to configure these test parameters on both the generator (local) switch and the analyzer (remote) switch for the specified CPE test.

test-oam *string* **[vlan** *svlan***] [[test-frame [src-mac** *src-address***] [dst-mac** *dst-address***]]**

Syntax Definitions

string	The name of an existing CPE test.
svlan	The service VLAN ID. This is used for traffic analysis and test-frame accounting.
src-address	Source mac-address of the test-frame.
dst-address	Destination mac-address of the test-frame.

Defaults

parameter	default
src-address	00:00:00:00:00:00
dst-address	00:00:00:00:00:00

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Although the source and destination MAC addresses are optional parameters with this command, the test will not run if these addresses are set to all zeros (the default).
- Make sure that routing is disabled on the specified SVLAN.
- Avoid configuring any IEEE reserved MAC addresses as the destination MAC address for the test.
- This command automatically overwrites the SVLAN, source MAC, or destination MAC values previously configured for the specified CPE test.

Examples

```
-> test-oam Test1 vlan 100 test-frame src-mac 00:01:02:00:00:02 dst-mac
00:00:01:00:00:90
-> test-oam Test1 vlan 100
-> test-oam Test1 test-frame src-mac 00:01:02:00:00:02 dst-mac 00:00:01:00:00:90
-> test-oam Test1 test-frame src-mac 00:01:02:00:00:02
-> test-oam Test test-frame dst-mac 00:00:01:00:00:90
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam role	Configures the switch as a generator or analyzer for the test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigVlan
   alaTestOamConfigFrameSrcMacAddress
   alaTestOamConfigFrameDstMacAddress
```

test-oam role

Configures the role the switch will perform for the specified CPE test. The type of role assigned determines whether the switch transmits (generator) or receives (analyzer) or loopback test frames.

test-oam *string* **role {generator | analyzer | loopback}**

Syntax Definitions

string	The name of an existing CPE test.
generator	Configures the switch as the test generator.
analyzer	Configures the switch as the test analyzer.
loopback	Configures the switch as loopback.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use this command on the switch that will perform the specified role.
- Configuring a generator and an analyzer switch for each test is required.
- Only one role can be assigned to the switch for a particular test.
- This command automatically overwrites the previously configured switch role for the specified CPE test.

Examples

```
-> test-oam Test1 role generator
-> test-oam Test2 role analyzer
-> test-oam Test2 role loopback
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam duration rate packet-size	Configures the test frame duration, rate and packet-size for the test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigRole
```

test-oam duration rate packet-size

Configures the duration, rate, and packet-size for the specified test. Use this command to configure these test parameters on the generator switch.

test-oam *string* **[duration** *secs***] [rate** *rate***] [packet-size** *bytes***]**

Syntax Definitions

string	The name of an existing CPE test.
secs	The duration of the test, in seconds. This is the amount of time the generator will actively transmit test packets to the remote (analyzer) switch. The valid time range is 1–3600 seconds
rate	The rate, in Kbps or Mbps, at which test traffic is generated. The minimum value allowed is 8 Kbps to line rate. The granularity of the transmit rate is 8 Kbps for 100 Mbps port and 2 Mbps for 1Gig ports.
bytes	The packet size, in bytes. The valid range is 64–9212 bytes.

Defaults

Parameter	Default
secs	5 secs
rate	8 k
bytes	64 byte

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- This command automatically overwrites any duration, rate, and packet size parameter values previously configured for the specified CPE test.
- The status of the CPE test will change to “ended” when the test duration time expires.
- This command automatically overwrites the duration, rate, or packet size values previously configured for the specified CPE test.

Examples

```
-> test-oam Test1 duration 10 rate 8k packet-size 64
-> test-oam Test1 rate 8m
-> test-oam Test1 duration 10
-> test-oam Test1 packet-size 64
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam frame	Configures the test frame parameter values for the CPE test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigDuration
   alaTestOamConfigGeneratorBandwidth
   alaTestOamConfigGeneratorPacketSize
```

test-oam frame

Configures the test frame parameter values for the specified CPE test. Use this command on the switch that will generate the test frame traffic.

test-oam *string* **frame**
[vlan-tag *vlan-id* **priority** *priority* **drop-eligible {true | false}}]**
ether-type {*hex-num* | **ipv4 {src-ip** *src-ipv4* **dst-ip** *dst-ipv4* **[ttl** *ttl***] [tos** *tos***] [protocol {udp | tcp} {src-port** *src-port* **dst-port** *dst-port***}]}]} [data-pattern** *pattern***]**

Syntax Definitions

string	The name of an existing CPE test.
vlan-id	The VLAN ID of the frame.
priority	The priority value. The valid range is 0–7.
true	Sets the drop-eligible bit to true.
false	Sets the drop-eligible bit to false.
hex-num	The hexadecimal ethertype value. The valid range is 0x600–0xfffe.
src-ipv4	The source IP address for an IPv4 test frame.
dst-ipv4	The destination IP address for an IPv4 test frame.
ttl	The time-to-live value. The valid range is 0–255.
tos	The type-of-service value for QoS features. The valid range is 0x0–0xff.
udp	Specifies the UDP protocol.
tcp	Specifies the TCP protocol.
src-port	The source port of the generated test frame.
dst-port	The destination port of the generated test frame.
pattern	The data pattern present in the generated test frame. The valid range is 0x0000–0xffff.

Defaults

Parameter	Default
priority	7
drop-eligible	false
ttl	64
tos	0x0
pattern	0x0000

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Specify the Ether type in hexadecimal format to configure a Layer 2 test frame.
- Specify **ipv4** as the Ether type to configure a Layer 3 test frame. When this option is selected, entering a source and destination IP address is required.
- Do not specify reserved Ether type values.
- This command automatically overwrites the test packet parameter values previously configured for the specified CPE test.

Examples

If the ether-type is a hexadecimal number (Layer 2 test frame):

```
-> test-oam Test1 frame vlan-tag 1 priority 2 drop-eligible false ether-type 0x0100
data-pattern 0x0010
```

If the ether-type is IPV4 (Layer 3 test frame):

```
-> test-oam Test1 frame vlan-tag 1 priority 2 drop-eligible false ether-type ipv4
src-ip 1.1.1.1 dst-ip 2.2.2.2 ttl 4 tos 0x01 protocol udp src-port 2000 dst-port
3000 data-pattern 0x0010
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam l2-saa	Start or stop the CPE test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
alaTestOamEtherConfigTable
alaTestOamIpv4ConfigTable
```

test-oam l2-saa

Configures to run SAA tests in parallel with test streams.

test-oam *string* **l2-saa [priority** *vlan-priority***] [count** *num-pkts***] [interval** *inter-pkt-delay***] [continuous] [size** *size***] [drop-eligible {true | false}]**

no test-oam *string* **l2-saa**

Syntax Definitions

string	The name of an existing CPE test.
vlan-priority	Specify the internal priority of MAC ping and 802.1p value on the VLAN tag header.
num-pkts	The number of packets sent in one ping iteration. Valid range is 1 to 10.
inter-pkt-delay	The delay between packets sent during a ping iteration (milliseconds). Valid range is 100 to 1000, in multiples of 100.
continuous	Allows the SAA session to run continuously until the test-oam session ends.
size	The payload size to be used for MAC ping iteration. Must be within 1500 bytes.
drop-eligible	Specify the drop precedence of the MAC ping and the Canonical Format Indicator (CFI) bit on the VLAN tag header.

Defaults

Parameter	Default
vlan-priority	0
num-pkts	5
inter-pkt-delay	1000 ms
size	36 bytes
drop-eligible	false

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- The L2-SAA test derives the source MAC, destination MAC, and the VLAN ID from the test OAM configuration of the individual test frames.
- The default L2-SAA configuration values will be applied if no optional parameters are configured.
- To run the L2-SAA session until the test-oam session ends, use the **continuous** parameter.
- Different SAA profiles can be configured for each individual test stream.

- Use the **no** form of this command to remove the L2-SAA configuration for the test.

Examples

```
-> test-oam test1 l2-saa priority 5 count 5 interval 1000 size 100 drop-eligible
false
-> test-oam test1 l2-saa continuous
-> no test-oam test1 l2-saa
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam	Configures the CPE test name and an optional description. The test name is used to identify and configure a CPE test profile.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamSaaConfigDropEligible
   alaTestOamSaaConfigPayloadSize
   alaTestOamSaaConfigNumPkts
   alaTestOamSaaConfigInterPktDelay
   alaTestOamSaaContinuous
```

test-oam start stop

Starts or stops the CPE test operation.

test-oam *string* **{[vlan** *vlan-id***] [port** *chassis/slot/port***] [packet-size** *bytes***] start | stop} [fetch-remote-stats]**

Syntax Definitions

string	The name of an existing CPE test.
vlan-id	The service VLAN ID. This value is required only for traffic analysis and test frame accounting and is not related to the VLAN tag specified for the actual test frame.
chassis/slot/port	The switch port on which the test is run.
bytes	The size of the test packet, in bytes. The valid packet size range is 64–9212 bytes.
start	Starts the CPE test operation.
stop	Stops the CPE test operation.
fetch-remote-stats	Triggers the test at the remote device from the generator. The statistics are collected from the remote device and the test is stopped after receiving the test results.

Defaults

Parameter	Default
bytes	64

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Ensure that routing is disabled on the specified service VLAN.
- The optional **vlan**, **port,** and **packet-size** parameters specify “active” parameter values that are applied when the specified CPE test is started. If these same parameters are defined within a CPE test profile, they are considered “configured” parameter values. Active parameter values override configured parameter values when the test is started.
- If no active parameter values are specified with this command, the test is started using the configured values defined in the CPE test profile. However, if active parameter values are not specified and the CPE test does not contain any configured values for these parameters, the test will not run.
- Specifying any of the optional parameter values does not change the configured values associated with the CPE test.
- If the specified port resides on a switch that will transmit test traffic, the port will generate the test frames. However, if the switch is an analyzer switch, specifying a port is not required.

- Start the specified test on the analyzer switch first and then on the generator switch.
- The test will stop when the test duration time expires or when the test is manually stopped using the **test-oam stop** command.
- Manually restart the test if the test is interrupted by a takeover, restart, or hot swap.
- The previous statistics related to the test will be cleared automatically once the test is started.
- Use the **fetch-remote-stats** parameter to collect the test statistics from the remote device. This parameter must be used to start the bidirectional test.

Examples

```
-> test-oam Test1 start
-> test-oam Test1 vlan 100 start
-> test-oam Test1 port 1/1/1 start
-> test-oam Test1 packet-size 100 start
-> test-oam Test1 vlan 100 port 1/1/1 packet-size 100 start
-> test-oam Test1 stop
-> test-oam Test1 start fetch-remote-stats
-> test-oam "test2" port 1/1/2 start fetch-remote-stats
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam statistics	Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigVlan
   alaTestOamConfigPort
   alaTestOamConfigGeneratorPacketSize
   alaTestOamConfigTestIdState
   alaTestOamConfigRemoteStatsFetch
```

test-oam remote-sys-mac

Configures the system MAC address of the remote device to receive test OAM messages.

test-oam *string* **remote-sys-mac** *string*

Syntax Definitions

string	The name of an existing CPE test.
remote-sys-mac	The system MAC address of the remote device.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use this command on the generator switch to set the system MAC address of the remote device to receive the test OAM messages.
- remote-sys-mac must be the primary CMM MAC address of the remote device. Use the **show cmm** command on the remote device to know the chassis MAC address of the device.
- remote-sys-mac is not applicable for analyzer or loopback.
- Configuring the Remote Sys MAC is mandatory for bidirectional test and optional for unidirectional test.

Examples

```
-> test-oam Test1 remote-sys-mac 00:e0:b1:7c:7a:fa
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigRemoteSysMacAddress
```

test-oam statistics flash-logging

Enable or disable the option to save the statistics of the test on the file in the flash directory of the switch. The test information is appended at the end of the default text file (testoamActiveStats.txt) in the flash.

test-oam statistics flash-logging {enable | disable}

Syntax Definitions

N/A

Defaults

Parameter	Default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465

Usage Guidelines

Use the **more** command to read the test results stored on the switch.

Examples

```
-> test-oam statistics flash-logging enable
-> test-oam statistics flash-logging disable
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam statistics	Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.
show test-oam saa statistics	Clears the statistics for all CPE tests or for a specific test name.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigStatsSave
```

show test-oam

Displays the CPE test configuration and status.

show test-oam [tests | *string***]**

Syntax Definitions

tests	Displays information for all the CPE tests**.**
string	The name of an existing CPE test.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the **tests** parameter to display information for all CPE tests configured on the switch.
- Use the *string* parameter to display detailed information for a specific CPE test.

Examples

```
-> show test-oam tests
Total Test-Ids: 1
Test-Id Port       Src-Mac        Dst-Mac         Vlan     Direction     Status         Remote-Sys-Mac
-------+-----+-----------------+-----------------+-----+--------------+-----------+----------------------
Test1   none  00:00:00:00:00:00  00:00:00:00:00:00 none  unidirectional  not-started  00:00:00:00:00:00
```

output definitions

Test-Id	The CPE test name (ID). Configured through the **test-oam** command.
Port	The port on which the test is run. Configured through the **test-oam port** command.
Src-Mac	The source MAC address of the test frame. Configured through the **test-oam vlan test-frame** command.
Dst-Mac	The destination MAC address of the test frame. Configured through the **test-oam vlan test-frame** command.
Vlan	The service VLAN (SVLAN) associated with the test. Configured through the **test-oam vlan test-frame** command.
Direction	The direction of the test traffic. Note that only unidirectional traffic tests are supported.
Status	The operational status of the test.
Remote-Sys-Mac	The MAC address of the remote device configured through the **test-oam remote-sys-mac** command.

```
-> show test-oam Test1
Legend: dei-drop eligible indicator
TEST Parameters for Test1:
  Source Endpoint      : SW1,
  Destination Endpoint : SW2,
  Test Description     : Ether Test,
  Direction            : unidirectional,
  Source MAC           : 00:11:22:33:44:55,
  Destination MAC      : 00:22:33:44:55:66,
  Remote Sys MAC       : E8:E7:32:72:01:A4,
  Duration             : 10(secs),
  Vlan                 : 100,
  Role                 : generator,
  Port                 : 1/1,
  Tx Rate              : 80m,
  Frame Size           : 100,
  State                : start,
  Status               : running

Frame Configuration:
  Frame Type : ether,
  Vlan       : 200,
  Priority   : 7,
  Pattern    : 0x0001,
  Dei        : none,
  Ether Type : 0x8000,

-> show test-oam Test2
TEST Parameters for Test2:
  Source Endpoint      : SW1,
  Destination Endpoint : SW2,
  Test Description     : IPV6 Test,
  Direction            : unidirectional,
  Source MAC           : 00:11:22:33:44:55,
  Destination MAC      : 00:22:33:44:55:66,
  Remote Sys MAC       : E8:E7:32:72:01:A4,
  Duration             : 10(secs),
  Vlan                 : 100,
  Role                 : generator,
  Port                 : 1/1,
  Tx Rate              : 8k,
  Frame Size           : 100,
  State                : start,
  Status               : running

    Frame Configuration :
      Frame Type       : ipv6,
      Vlan             : 200,
      Priority         : 7,
      Pattern          : 0x0001,
      Dei              : true,
      Source Ip        : 00:00:00:00:10.20.30.50,
      Destination Ip   : 00:00:00:00:10.30.40.60,
      Source Port      : 10,
      Destination Port : 20,
      Next Header      : tcp,
      Hop-Count        : 50,
      Traffic-Class    : 0xff
      Flow-Label       : 0x0
```

```
L2-SAA Configuration  :
  L2-SAA DE           : False,
  L2-SAA Payload Size : 64,
  L2-SAA Count        : 0,
  L2-SAA Interval     : 1000,
  L2-SAA Continuous    : yes
  L2-SAA Priority     : 0
```

output definitions

Source Endpoint	The host name for the source (generator) switch. Configured through the **test-oam direction** command.
Destination Endpoint	The host name for the destination (analyzer) switch. Configured through the **test-oam direction** command.
Test Description	Description for the test name. Configured through the **test-oam** command.
Direction	The direction of the test traffic. Note that only unidirectional traffic tests are supported.
Source MAC	The source MAC address for the test frame. Configured through the **test-oam vlan test-frame** command.
Destination MAC	The destination MAC address for the test frame. Configured through the **test-oam vlan test-frame** command.
Remote Sys MAC	The MAC address of the remote device configured through the **test-oam remote-sys-mac** command.
Duration	The amount of time the test will run. Configured through the **test-oam duration rate packet-size** command.
Vlan	The service VLAN (SVLAN) associated with the test. Configured through the **test-oam vlan test-frame** command.
Role	The role of the switch for this test (**generator** or **analyzer**). Configured through the **test-oam role** command
Port	The port on which the test is run. Configured through the **test-oam port** command.
Tx Rate	The rate at which packets are transmitted on the test port. Configured through the **test-oam duration rate packet-size** command.
Frame Size	The size of the test frame. Configured through the **test-oam duration rate packet-size** command.
State	The administrative state of the test (**stop** or **start**). Configured through the **test-oam l2-saa** command.
Status	The operational status of the test (**running**, **ended**, **stopped**, or **not started**).
Frame Configuration	The test frame type (**ether** or **ipv4**) and associated parameter values. Configured through the **test-oam frame** command.
L2-SAA Configuration	Displays the L2 SAA configuration.

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam statistics	Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestId
   alaTestOamConfigPort
   alaTestOamConfigFrameSrcMacAddress
   alaTestOamConfigFrameDstMacAddress
   alaTestOamConfigVlan
   alaTestOamConfigDirection
   alaTestOamConfigTestIdStatus
   alaTestOamConfigRemoteSysMacAddress

alaTestOamSaaConfigTable
   alaTestOamSaaConfigDropEligible
   alaTestOamSaaConfigPayloadSize
   alaTestOamSaaConfigNumPkts
   alaTestOamSaaConfigInterPktDelay
   alaTestOamSaaConfigVlanPriority
   alaTestOamSaaContinuous

alaTestOamEtherConfigTable
   alaTestOamIpv4ConfigTable
```

show test-oam statistics

Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

show test-oam [*string***] statistics**

Syntax Definitions

string	The name of an existing CPE test.

Defaults

By default, statistics are displayed for all CPE tests.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the *string* parameter with this command to display statistics for a specific CPE test.
- The statistics displayed depend on the role the switch is performing for the test (generator or analyzer). For example, the analyzer switch may not show any packet count in the **TX** fields because it is the receiving switch.

Examples

```
-> show test-oam Test1 statistics

Test-Id   TX-Ingress   TX-Egress    RX-Ingress      Remote-Stats  Throughput(Mbps)
--------+------------+------------+---------------+--------------+---------------
Test1    19017        19017         19017             19017         9.98


-> show test-oam statistics
Test-Id      TX-Ingress   TX-Egress    RX-Ingress Remote-Stats Throughput(Mbps)
------------+------------+------------+----------+------------+---------------
Test1        1200366      1200366          0       1200366      8
Test2          0             0          1200366    1200366      8
```

output definitions

Test-Id	The CPE test name (ID).
TX-Ingress	The number of ingress test packets generated on the ingress UNI.
TX-Egress	The number of egress test packets transmitted on the egress NNI.
RX-Ingress	The number of test packets received on the ingress NNI. This value is relevant on the receiving (analyzer) switch for the specific test.

output definitions

Remote-Stats	The number of test frames received by the analyzer and fetched by the generator device.
Throughput (Mbps)	Displays the traffic throughput of the test.

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam statistics flash-logging	Displays the CPE test configuration and status.
clear test-oam statistics	Clears CPE test statistics.

MIB Objects

```
alaTestOamStatsTable
   alaTestOamConfigTestId
   alaTestOamTxIngressCounter
   alaTestOamTxEgressCounter
   alaTestOamRxIngressCounter
   alaTestOamRemoteStatsCounter
   alaTestOamBandwidthThroughputStr
```

show test-oam saa statistics

Displays the SAA test statistics for all CPE tests or for a specific test name.

show test-oam [*string*] saa statistics

Syntax Definitions

string	The name of an existing CPE test.

Defaults

By default, statistics are displayed for all CPE tests.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

Use the *string* parameter with this command to display SAA statistics for a specific CPE test.

Examples

```
-> show test-oam Test1 saa statistics

Test    Time of Last-Run       RTT    RTT    RTT   Jitter Jitter Jitter  Packets    Description
                               Min    Avg    Max    Min    Avg    Max   Sent Rcvd
-----+----------------------+-------+------+-----+------+------+------+----+------+-------------
Test1   2009-09-05,20:18:34.0  970    1067   1432    1    99      455    7    7      DEFAULT


-> show test-oam saa statistics
Test    Time of Last-Run       RTT    RTT    RTT   Jitter Jitter Jitter  Packets    Description
                               Min    Avg    Max    Min    Avg    Max   Sent Rcvd
-----+----------------------+------+----+-------+------+-------+-----+----+------+------------
Test1   2009-09-05,20:18:34.0  970    1067   1432    1    99      455    7    7      DEFAULT
Test2   2009-09-05,30:28:34.0  770    865    1432    2    99      255    7    7      DEFAULT
Test3   2009-09-05,40:38:34.0  570    967    1432    3    99      355    7    7      DEFAULT
Test4   2009-09-05,50:48:34.0  770    807    1432    1    99      255    7    7      DEFAULT
Test5   2009-09-06,20:18:34.0  640    867    1432    2    99      445    7    7      DEFAULT
Test6   2009-09-06,30:18:34.0  780    907    1432    3    99      255    7    7      DEFAULT
```

output definitions

Test	The CPE test name (ID).
Time of Last-Run	Displays the date and time on which the test was last run.
RTT Min	Displays the minimum round trip time.
RTT Avg	Displays the average round trip time.
RTT Max	Displays the maximum round trip time.
Jitter Min	Displays the minimum jitter value.
Jitter Avg	Displays the average jitter value.
Jitter Max	Displays the maximum jitter value.

output definitions

Packets Sent	Displays the number of packets sent during a single MAC ping.
Packets Rcvd	Displays the number of packets received during a single MAC ping.
Description	Displays the Test Description parameter value for each test

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam statistics flash-logging	Displays the CPE test configuration and status.
clear test-oam statistics	Clears CPE test statistics.

MIB Objects

```
alaTestOamSaaStatsTable
   alaTestOamConfigTestId
   alaTestOamSaaRunTime
   alaTestOamSaaPktsSent
   alaTestOamSaaPktsRcvd
   alaTestOamSaaMinRTT
   alaTestOamSaaAvgRTT
   alaTestOamSaaMaxRTT
   alaTestOamSaaMinJitter
   alaTestOamSaaAvgJitter
   alaTestOamSaaMaxJitter
```

clear test-oam statistics

Clears the statistics for all CPE tests or for a specific test name.

clear test-oam [*string***] statistics**

Syntax Definitions

string	The name of an existing CPE test.

Defaults

By default, statistics are cleared for all CPE tests.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

Use the *string* parameter with this command to clear the statistics for a specific CPE test.

Examples

```
-> clear test-oam Test1 statistics
-> clear test-oam statistics
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam statistics	Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.
show test-oam saa statistics	Displays the SAA test statistics for all CPE tests or for a specific test name.

MIB Objects

```
alaTestOamStatsTable
   alaTestOamConfigTestId
   alaTestOamStatsClearStats
```

test-oam group

Configures the CPE test group name and an optional description. The group name is used to identify and configure a CPE test group.

test-oam group *string* **[descr** *description***]**

no test-oam group *string*

Syntax Definitions

string	The name of the CPE test group, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test-oam group.
description	The description to assign to the CPE test group, an alphanumeric string between 1 and 32 characters.

Defaults

parameter	default
description	DEFAULT

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the **no** form of this command to remove the specified CPE test group.
- This command creates a CPE test group that is identified by the test-oam name. Make sure the name specified does not exist in the switch configuration.
- To configure a CPE test group, the individual test must be configured.
- A maximum of four tests can be configured to run concurrently.
- Only one CPE test group can be active on the switch at any given time.

Examples

```
-> test-oam group Testgroup1
-> test-oam group Testgroup2 descr second-testgroup
-> no test-oam group Testgroup1
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group statistics	Displays the statistics for all CPE test groups or for a specific CPE test group. Use this command on both the generator and analyzer switch to determine test results.
show test-oam group	Displays the statistics for all CPE test groups or for a specific CPE test group.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamConfigGroupDescription
   alaTestOamGroupConfigRowStatus
```

test-oam group tests

This defines the list of CPE test group tests that need to be added in the test-oam group.

test-oam group *string* **[tests** *string1.....string8***]**

test-oam group *string* **[no tests** *string1.....string8***]**

Syntax Definitions

string	The name of the CPE test group, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test group.
string1.....string8	The name of the configured test-oam tests.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- This command defines the list of test-oam tests that need to run concurrently.
- The test must exist, while configuring the test-oam list.
- A maximum of four tests can be configured to run concurrently.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of test-oam group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.
- use the **no** form of the command to remove the test-oam tests from the CPE test group.

Examples

```
-> test-oam test1
-> test-oam test2
-> test-oam test3
-> test-oam test4
-> test-oam test5
-> test-oam test6
-> test-oam test7
-> test-oam test8
-> test-oam group Testgroup1 descr first-testgroup
-> test-oam group Testgroup1 tests test1 test2 test3 test4 test5 test6 test7 test8
-> test-oam group Testgroup1 no tests test1 test2 test3
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
show test-oam group	Displays the SAA statistics for all CPE test groups or for a specific CPE test group if mentioned.

MIB Objects

```
alaTestOamGroupFlowConfigTable
   alaTestOamConfigGroupId
   alaTestOamConfigTestId
   alaTestOamGroupFlowConfigRowStatus
```

test-oam feeder

This configures the feeder port globally in the system for CPE test group to feed the test traffic to generator port.

test-oam feeder-port *chassis/lot/port*

no test-oam feeder-port

Syntax Definitions

chassis/slot/port	The port to be used to feed the test traffic only to generator port.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- This command configures the feeder port globally in the system.
- The feeder port cannot be the generator port and the generator port cannot be the feeder port.
- When a CPE test group is running, the modification to the feeder port shall not be allowed.
- use the **no** form of the command to remove the feeder port from the system for CPE test group.

Examples

```
-> test-oam feeder-port 1/1/4
-> no test-oam feeder-port
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam group port	Configures the port on which the CPE test group will run.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGlobalFeederPort
```

test-oam group src-endpoint dst-endpoint

Configures the source and destination endpoints for the CPE test group.

test-oam group *string* **[src-endpoint** *src-string* **dst-endpoint** *dst-string***] [src-endpoint** *src-string***] [dst-endpoint** *dst-string***]**

Syntax Definitions

string	The name of an existing CPE test group.
src-string	The management IP address or DNS host name of the switch that will transmit test traffic.
dst-string	The management IP address or DNS host name of the switch that will receive test traffic. This is the switch on which traffic analysis is done.

Defaults

parameter	default
src-endpoint	DEFAULT
dst-endpoint	DEFAULT

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Using the DNS host name of the switch is highly recommended, as this name is unique and is mapped to an IP address configured for the switch.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of test-oam group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 src-endpoint SW1 dst-endpoint SW2
-> test-oam group Testgroup1 src-endpoint SW1
-> test-oam group Testgroup1 dst-endpoint SW2
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam group duration rate	Configures the duration and rate for the specified CPE test group.

show test-oam group Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigSourceEndpoint
   alaTestOamGroupConfigDestinationEndpoint
```

test-oam group role

Configures the role the switch will perform for the specified CPE test group. The type of role assigned determines whether the switch transmits (generator) or receives (analyzer) test frames.

test-oam group *name* **role {generator | analyzer | loopback}**

Syntax Definitions

name	The name of an existing CPE test group.
generator	Configures the switch as the test generator.
analyzer	Configures the switch as the test analyzer.
loopback	Configures the switch as loopback.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 role generator
-> test-oam group Testgroup2 role analyzer
-> test-oam group Testgroup2 role loopback
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam group duration rate	Configures the duration and rate for the specified CPE test group.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigRole
```

test-oam group port

Configures the port on which the CPE test group will run. Use this command on the switch that will generate the test traffic.

test-oam group *string* **port** *chassis/slot/port*

Syntax Definitions

string	The name of an existing CPE test group.
chassis/slot/port	The port on which the CPE test will generate traffic.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Configuring a port that is not in use is recommended. In addition, if the test port is a UNI port associated with an SAP profile, only that UNI port is used for the test. Traffic on other UNI ports associated with the same profile is *not* disrupted by the CPE test.
- This command automatically overwrites the port value previously configured for the specified CPE test group.
- The feeder port cannot be the generator port and the generator port cannot be the feeder port.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 port 1/1/2
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam group start stop	Starts the traffic test for the CPE test group on the configured port or the given port.
test-oam group remote-sys-mac	Stops the traffic test for the CPE test group on the configured port or the given port.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
```

test-oam group direction

Configures the test direction of the test-oam group.

test-oam group *string* **[direction {unidirectional | bidirectional}]**

Syntax Definitions

string	The name of an existing CPE test group.
direction	The direction of the CPE test group.

Defaults

parameter	default
direction	unidirectional

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 direction unidirectional
-> test-oam group Testgroup2 direction bidirectional
```

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam group duration rate	Configures the duration and rate for the specified CPE test group.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigDirection
```

test-oam group duration rate

Configures the duration and rate for the specified test-oam group. Use this command to configure these test parameters on the generator switch.

test-oam group *string* **[duration** *secs***] [rate** *rate***]**

Syntax Definitions

string	The name of an existing CPE test group.
secs	The duration of the test, in seconds. This is the amount of time the generator will actively transmit test packets to the remote (analyzer) switch. The valid time range is 5–3600 seconds.
rate	The rate, in Kbps or Mbps, at which test traffic is generated. The minimum value allowed is 8 Kbps to line rate. The granularity of the transmit rate is 8 Kbps for 100 Mbps port and 2 Mbps for 1Gig ports.

Defaults

Parameter	Default
secs	5 secs
rate	8 k

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- This command automatically overwrites any duration and rate parameter values previously configured for the specified CPE test group.
- The status of the CPE test group will change to “ended” when the test duration time expires.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 duration 10
-> test-oam group Testgroup1 rate 8m
-> test-oam group Testgroup1 duration 10 rate 8m
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigDuration
   alaTestOamGroupConfigGeneratorBandwidth
```

test-oam group start stop

Starts or stops the traffic test for the test-oam group on the configured port or the given port.

test-oam group *string* **{[port** *chassis/slot/port***] start | stop} [fetch-remote-stats]**

Syntax Definitions

string	The name of an existing CPE test group.
chassis/slot/port	The port on which the CPE test group will generate traffic.
start	Enables the test.
stop	Disables the test.
fetch-remote-stats	Triggers the group test at the remote device from the generator. The statistics are collected during the test and the test is stopped after receiving the test results.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.
- Use the fetch-remote-stats parameter to collect the test statistics from the remote device.

Examples

```
-> test-oam group Testgroup1 port 1/1/2 start
-> test-oam group Testgroup2 start
-> test-oam group Testgroup1 start fetch-remote-stats
-> test-oam group testgroup2 port 1/1/2 start fetch-remote-stats
-> test-oam group Testgroup1 stop
-> test-oam group Testgroup2 stop
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
   alaTestOamGroupConfigState
   alaTestOamGroupConfigRemoteStatsFetchState
```

test-oam group remote-sys-mac

Configures the system MAC address of the remote device to receive test OAM messages.

test-oam group *string* **remote-sys-mac** *string*

Syntax Definitions

string	The name of an existing CPE test group.
remote-sys-mac	The system MAC address of the remote device.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use this command on the switch to set the system MAC address of the remote device to receive the test OAM messages.
- remote-sys-mac must be the primary CMM MAC address of the remote device.
- remote-sys-mac is not applicable for analyzer or loopback.

Examples

```
-> test-oam group Testgroup1 remote-sys-mac 00:e0:b1:7c:7a:fa
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamGroupConfigRemoteSysMacAddress
```

clear test-oam group statistics

This clears the statistics of the CPE test group.

clear test-oam group *string* **statistics**

Syntax Definitions

string	The name of an existing CPE test group.
statistics	Clears the statistics for the give CPE test group.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> clear test-oam group Testgroup1 statistics (Clears the statistics for the
specified test-oam group)
-> clear test-oam group statistics (Clears the statistics for all the test-oam
groups)
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group statistics	Displays the statistics for all test-oam groups or for a specific CPE test group.
show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigStatsClear
   alaTestOamGlobalGroupClearStats
```

show test-oam group

Displays the configuration and status of the CPE test groups.

show test-oam group [tests | *string***]**

Syntax Definitions

tests	Displays information for all the CPE test groups**.**
string	The name of an existing CPE test group.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the **tests** parameter to display information for all CPE test groups configured on the switch.
- Use the *string* parameter to display detailed information for a specific CPE test group.

Examples

```
-> show test-oam group tests

Total Test-Groups: 2
Feeder Port      : none
Test-Group  Port  Duration     Rate    Nb of   Direction      Status        Remote-Sys-Mac
                   (secs)             Flows
----------+-----+----------+---------+-----+--------------+------------+--------------------
Testgroup1 none    5          -         2    unidirectional  not-started  00:00:00:00:00:00
Testgroup2 none    5          -         3    unidirectional  not-started  00:00:00:00:00:00
```

output definitions

Test-Groups	The CPE test group. Configured through the **test-oam group** command.
Port	The port on which the test is run.
Duration	The amount of time the test will run.
Rate	The rate at which packets are transmitted on the test port. Configured through the **test-oam group duration rate** command.
Nb of Flows	Number of test flows configured for the respective CPE test group.
Direction	The direction of the test traffic. Note that only unidirectional traffic tests are supported.
Status	The operational status of the test.
Remote-Sys-Mac	The MAC address of the remote device configured through the **test-oam group remote-sys-mac** command.

```
-> show test-oam group Testgroup1
Legend: Port: * = Inactive port

TEST Parameters for Testgroup1:
  Source Endpoint         : SW1,
  Destination Endpoint    : SW2,
  Test Group Description  : first-testgroup,
  Direction               : bidirectional,
  Role                    : generator,
  Tx Rate                 : 10m,
  Duration                : 60 (secs),
  Port                    : 1/5,
  State                   : stop,
  Status                  : not-started,
  Remote Sys MAC          : E8:E7:32:32:A6:EE
    Flow 1:
      Test Name           : test1,
      Vlan                : 1001,
      Tx Rate             : 10m,
      Source MAC          : 00:11:22:12:44:55,
      Destination MAC     : 00:22:33:12:55:66,
      Remote Sys MAC      : E8:E7:32:32:A6:EE,
      Frame Size          : 64,
      L2-SAA DE           : False,
      L2-SAA Payload Size : 64,
      L2-SAA Count        : 5,
      L2-SAA Interval     : 1000,
      L2-SAA Priority     : 0
      L2-SAA Continuous   : no
    Flow 2:
      Test Name           : test2,
      Vlan                : 1001,
      Tx Rate             : 10m,
      Source MAC          : 00:11:22:13:44:55,
      Destination MAC     : 00:22:33:13:55:66,
      Remote Sys MAC      : E8:E7:32:32:A6:EE,
      Frame Size          : 100,
      L2-SAA DE           : True,
      L2-SAA Payload Size : 120,
      L2-SAA Count        : 0,
      L2-SAA Interval     : 900,
      L2-SAA Priority     : 6
      L2-SAA Continuous   : yes
    Flow 3:
      Test Name           : test3,
      Vlan                : 1001,
      Tx Rate             : 10m,
      Source MAC          : 00:11:22:14:44:55,
      Destination MAC     : 00:22:33:14:55:66,
      Remote Sys MAC      : E8:E7:32:32:A6:EE,
      Frame Size          : 100,
      L2-SAA DE           : True,
      L2-SAA Payload Size : 120,
      L2-SAA Count        : 0,
      L2-SAA Interval     : 900,
      L2-SAA Priority     : 6
      L2-SAA Continuous   : yes
    Flow 4:
      Test Name           : test4,
```

```
Vlan                : 1001,
Tx Rate             : 10m,
Source MAC          : 00:11:22:15:44:55,
Destination MAC     : 00:22:33:15:55:66,
Remote Sys MAC      : E8:E7:32:32:A6:EE,
Frame Size          : 100
L2-SAA DE           : True,
L2-SAA Payload Size : 120,
L2-SAA Count        : 0,
L2-SAA Interval     : 900,
L2-SAA Priority     : 6
L2-SAA Continuous   : yes
```

output definitions

Test-Groups	The CPE test group. Configured through the **test-oam group** command.
Port	The port on which the test is run.
Source Endpoint	The host name for the source (generator) switch. Configured through the **test-oam group src-endpoint dst-endpoint** command.
Destination Endpoint	The host name for the destination (analyzer) switch. Configured through the **test-oam group src-endpoint dst-endpoint** command.
Source Mac	The source MAC address of the test frame. Configured through the **test-oam vlan test-frame** command.
Destination Mac	The destination MAC address of the test frame. Configured through the **test-oam vlan test-frame** command.
Remote Sys Mac	The MAC address of the remote device configured through the **test-oam group remote-sys-mac** command.
Duration	The amount of time the test will run.
Role	The role of the switch for this test (**generator** or **analyzer**). Configured through the **test-oam role** command.
Rate	The rate at which packets are transmitted on the test port. Configured through the **test-oam group duration rate** command.
Frame Size	The size of the test frame. Configured through the **test-oam group duration rate** command.
Direction	The direction of the test traffic. Note that only unidirectional traffic tests are supported.
Status	The operational status of the test.
L2-SAA Count	Specifies the number of packets sent in one MAC ping iteration.
L2-SAA Interval	Specifies the delay between two consecutive packets transmitted during a MAC ping iteration.
L2-SAA DE	Specifies if the drop enable bit value is used.
L2-SAA Payload Size	Specifies the size of the MAC ping payload used for the MAC ping operation.
L2-SAA Priority	Specifies the priority value set for the L2 SAA frames.
L2-SAA Continuous	Specifies the SAA session will run continuously until the test-oam session ends.

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group	Displays the statistics for all CPE test groups or for a specific CPE test group.

MIB Objects

```
alaTestOamGloabalFeederPort
alaTestOamGroupConfigTable
alaTestOamGroupConfigRowStatus
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
   alaTestOamGroupConfigDuration
   alaTestOamGroupConfigGeneratorBandwidth
   alaTestOamGroupConfigFlowCount
   alaTestOamGroupConfigDirection
   alaTestOamGroupConfigStatus
   alaTestOamGroupConfigRemoteStatsFetchState
   alaTestOamGroupConfigRemoteSysMacAddress
alaTestOamGroupConfigTable
     alaTestOamConfigGroupId
     alaTestOamGroupConfigSourceEndpoint
     alaTestOamGroupConfigDestinationEndpoint
     alaTestOamConfigGroupDescription
     alaTestOamGroupConfigDirection
     alaTestOamGroupConfigRole
     alaTestOamGroupConfigGeneratorBandwidth
     alaTestOamGroupConfigDuration
     alaTestOamGroupConfigPort
     alaTestOamGroupConfigState
     alaTestOamGroupConfigStatus
    alaTestOamGroupConfigStatsClear

  alaTestOamGroupFlowConfigTable
    alaTestOamConfigTestId
    alaTestOamGroupFlowVlan
    alaTestOamConfigGroupId
    alaTestOamGroupFlowGeneratorBandwidth
    alaTestOamGroupFlowFrameSrcMacAddress
    alaTestOamGroupFlowFrameDstMacAddress
    alaTestOamGroupFlowGeneratorPacketSize
```

show test-oam group saa statistics

Displays the SAA test statistics for all CPE test groups or for a specific test name.

show test-oam group [*string*] saa statistics

Syntax Definitions

string	The name of an existing CPE test group.

Defaults

By default, statistics are displayed for all CPE test group.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

Use the *string* parameter with this command to display SAA statistics for a specific CPE test group.

Examples

```
-> show test-oam group Test1 saa statistics

Test-group Flow Time of Last-Run       RTT    RTT    RTT   Jitter Jitter Jitter  Packets    Description
                                       Min    Avg    Max    Min    Avg    Max   Sent Rcvd
---------+-----+--------------------+-------+------+-----+------+------+------+----+------+-------------
Test1     flow1 2009-09-05,20:18:34.0  970    1067   1432    1    99      455    7    7      DEFAULT


-> show test-oam group saa statistics

Latest Record:
Test-group Flow Time of Last-Run       RTT    RTT    RTT   Jitter Jitter Jitter  Packets    Description
                                       Min    Avg    Max    Min    Avg    Max   Sent Rcvd
---------+-----+--------------------+------+-----+-------+-----+------+-----+-----+------+------------
Test1     flow1 2009-09-05,20:18:34.0  970    1067   1432    1    99      455    7    7      DEFAULT
Test2     flow2 2009-09-05,30:28:34.0  770    865    1432    2    99      255    7    7      DEFAULT
Test3     flow3 2009-09-05,40:38:34.0  570    967    1432    3    99      355    7    7      DEFAULT
Test4     flow4 2009-09-05,50:48:34.0  770    807    1432    1    99      255    7    7      DEFAULT
Test5     flow5 2009-09-06,20:18:34.0  640    867    1432    2    99      445    7    7      DEFAULT
Test6     flow6 2009-09-06,30:18:34.0  780    907    1432    3    99      255    7    7      DEFAULT
```

output definitions

Test-group	The CPE test group name (ID).
Flow	Displays the flow identifier for the test.
Time of Last-Run	Displays the date and time on which the test was last run.
RTT Min	Displays the minimum round trip time.
RTT Avg	Displays the average round trip time.
RTT Max	Displays the maximum round trip time.
Jitter Min	Displays the minimum jitter value.

output definitions

Jitter Avg	Displays the average jitter value.
Jitter Max	Displays the maximum jitter value.
Packets Sent	Displays the number of packets sent during a single MAC ping.
Packets Rcvd	Displays the number of packets received during a single MAC ping.
Description	Displays the description for each provided by the user during the test creation. By default it is displayed as “DEFAULT”.

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
clear test-oam group statistics	This clears the statistics of the CPE test group.

MIB Objects

```
alaTestOamGroupFlowSaaStats
   alaTestOamConfigGroupId
   alaTestOamConfigTestId
   alaTestOamGroupFlowSaaStatsEntry
   alaTestOamGroupFlowSaaRunTime
   alaTestOamGroupFlowSaaPktsSent
   alaTestOamGroupFlowSaaPktsRcvd
   alaTestOamGroupFlowSaaRunTime
   alaTestOamGroupFlowSaaMinRTT
   alaTestOamGroupFlowSaaAvgRTT
   alaTestOamGroupFlowSaaMaxRTT
   alaTestOamGroupFlowSaaMinJitter
   alaTestOamGroupFlowSaaAvgJitter
   alaTestOamGroupFlowSaaMaxJitter
```

show test-oam group statistics

Displays the statistics for all CPE test groups or for a specific CPE test group. Use this command on both the generator and analyzer switch to determine test results.

show test-oam group [*string***] statistics**

Syntax Definitions

string	The name of an existing CPE test group.

Defaults

By default, statistics are displayed for all CPE test groups.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Use the *string* parameter with this command to display statistics for a specific CPE test group.
- The statistics displayed depend on the role the switch is performing for the test (generator or analyzer). For example, the analyzer switch may not show any packet count in the **TX** fields because it is the receiving switch.

Examples

```
-> show test-oam group TestGroup4 statistics
Test-Group   Flow     TX-Ingress    TX-Egress       RX-Ingress   Remote-Stats
-----------+--------+-------------+---------------+------------+-----------
TestGroup4   flow1     19017         19017             0           19017
TestGroup4   flow2     19017         19017             0           19017

-> show test-oam group statistics
Test-Group Flow   TX-Ingress   TX-Egress    RX-Ingress    Remote-Stats  Throughput(Mbps)
----------+-----+------------+------------+-------------+-------------+---------------
Testgroup1 test1   20163463     17205475            0      17205475          172.05
Testgroup1 test2   20720137     17680541            0      17680541          176.81
Testgroup1 test3   20709603     17668483            0      17668483          176.68
Testgroup1 test4   20698156     17656987            0      17656987          176.57
Testgroup2 test1   20163463     17205475            0      17205475          172.05
Testgroup2 test2   20720137     17680541            0      17680541          176.81
Testgroup2 test3   20709603     17668483            0      17668483          176.68
Testgroup2 test4   20698156     17656987            0      17656987          176.57
```

output definitions

Test-Group	The CPE test group.
TX-Ingress	The number of ingress test packets generated on the ingress UNI.
TX-Egress	The number of egress test packets transmitted on the egress NNI.

output definitions

RX-Ingress	The number of test packets received on the ingress NNI. This value is relevant on the receiving (analyzer) switch for the specific test.
Remote-Stats	The number of test frames received by the analyzer and fetched by the generator device.
Throughput(Mbps)	Displays the traffic throughput of the test.

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
test-oam group remote-sys-mac	Clears the statistics of the CPE test group.

MIB Objects

```
alaTestOamGroupFlowStatsTable
   alaTestOamConfigGroupId
   alaTestOamConfigTestId
   alaTestOamGroupFlowTxIngressCounter
   alaTestOamGroupFlowTxEgressCounter
   alaTestOamGroupFlowRxIngressCounter
   alaTestOamGroupFlowRemoteStatsCounter
   alaTestOamGroupBandwidthThroughputStr
```

55 PPPoE Intermediate Agent

Point-to-Point Protocol over Ethernet (PPPoE) provides the ability to connect a network of hosts to a Remote Access Concentrator. For example, Broadband Network Gateway over a simple bridging access device. In PPPoE model, each host utilizes its own Point-to-Point Protocol (PPP) stack and the user is presented with a familiar user interface. By using PPPoE, Access control, billing, and type of service can be configured on a per-user, rather than a per-site, basis.

PPPoE Intermediate Agent (PPPoE-IA) solution is designed for the PPPoE access method and is based on the Access Node implementing a PPPoE-IA function to insert access loop identification in PPPoE discovery packets (PADI/PADR/PADT) received from the user side.

MIB information for the PPPoE-IA commands is as follows:

Filename: alcatel-ind1-pppoe-ia-mib.mib
Module: ALCATEL-IND1-PPPOEIA-MIB

A summary of the available commands is listed here.

pppoe-ia
pppoe-ia {port | linkagg}
pppoe-ia {trust | client}
pppoe-ia access-node-id
pppoe-ia circuit-id
pppoe-ia remote-id
clear pppoe-ia statistics
show pppoe-ia configuration
show pppoe-ia {port | linkagg}
show pppoe-ia statistics

Configuration procedures for PPPoE-IA are explained in the “Configuring PPPoE Intermediate Agent” chapter of the *OmniSwitch AOS Release 8 Network Configuration Guide*.

pppoe-ia

Enable or disable PPPoE-IA globally on the switch.

pppoe-ia {enable | disable}

Syntax Definitions

enable	Enable PPPoE-IA.
disable	Disable PPPoE-IA.

Defaults

By default, PPPoE-IA is disabled globally on the switch.

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

All PPPoE-IA parameters are configurable irrespective of the global status of PPPoE-IA.

Examples

```
-> pppoe-ia enable
-> pppoe-ia disable
```

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia {port | linkagg}	Enable or disable PPPoE-IA on a port or a link aggregate port.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
pppoe-ia access-node-id	Globally configures a format to form an identifier that uniquely identifies an access node.
pppoe-ia circuit-id	Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.
pppoe-ia remote-id	Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.
clear pppoe-ia statistics	Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAGlobalStatus
```

pppoe-ia {port | linkagg}

Enable or disable PPPoE-IA on a port or a link aggregate port. Link aggregate can be either static or dynamic.

pppoe-ia {port *chassis/slot/port*[*-port2*] **| linkagg** *agg_num***} {enable | disable}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for the module.
port	Port number of the interface to be configured.
port2	Last port number in a range of ports to be configured.
linkagg *agg_num*	The link aggregate identification number.
enable	Enable PPPoE-IA on a port.
disable	Disable PPPoE-IA on a port.

Defaults

By default, PPPoE-IA is disabled on all ports.

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

- All PPPoE-IA parameters are configurable irrespective of the per-port PPPoE-IA status (enabled or disabled).
- PPPoE-IA must be enabled globally as well as on a port.
- PPPoE-IA is not supported on port mirroring destination ports. However, the configurations are accepted.
- PPPoE-IA is not supported on aggregable ports.

Examples

```
-> pppoe-ia port 1/1/1 enable
-> pppoe-ia port 1/1/4 disable
-> pppoe-ia linkagg 1 enable
```

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAPortConfigTable
   alaPPPoEIAPortConfigStatus
```

pppoe-ia {trust | client}

Configures a port or a link aggregate port as trusted or client port for PPPoE-IA.

A trust port is a port that is connected to the Broadband Network Gateway whereas a client port is connected to the host.

pppoe-ia {port *chassis/slot/port*[*-port2*] **| linkagg** *agg_num***} {trust | client}**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for the module.
port	Port number of the interface to be configured.
port2	Last port number in a range of ports to be configured.
linkagg *agg_num*	Specifies the link aggregate identification number.
trust	Specifies the mode of the port as trust.
client	Specifies the mode of the port as client.

Defaults

By default, all ports are client ports.

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

- All PPPoE-IA parameters are configurable irrespective of per-port PPPoE-IA status (enabled or disabled).
- PPPoE-IA must be enabled globally as well as on a port.
- For PPPoE-IA to work, it must be enabled on a client port as well as a trusted port.
- PPPoE-IA is not supported on aggregable ports.
- PPPoE-IA is not supported on port mirroring destination ports; however, the configurations are accepted.

Examples

```
-> pppoe-ia port 1/1 /1
-> pppoe-ia port 1/1/2-4 client
-> pppoe-ia linkagg 7 trust
-> pppoe-ia linkagg 0 client
```

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {port | linkagg}	Enable or disable PPPoE-IA on a port or a link aggregate port.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAPortConfigTable
   alaPPPoEIAPortConfigTrustMode
```

pppoe-ia access-node-id

Globally configures a format to form an identifier that uniquely identifies an access node.

pppoe-ia access-node-id {base-mac | system-name | mgnt-address | user-string *string***}**

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The configured name of the switch.
mgnt-address	The IP address of the management interface of the switch.
string	The value of user configured string.

Defaults

By default, PPPoE-IA uses the base MAC address of the switch as the Access-Node-Identifier.

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

- The access-node-identifier can have a maximum of 32 characters. The access-node-identifier longer than 32 characters is truncated to 32 characters.
- The access-node-identifier when configured as user-string must not contain spaces.
- The value of user string must not be NULL.
- In case of management address format, IP address of the Loopback0 interface (if configured and active) or the first active IP interface address is used as the management address. If none of them are available, IP address ‘0.0.0.0’ is used as management address.
- If the access-node-identifier is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.

Examples

```
-> pppoe-ia access-node-id base-mac
-> pppoe-ia access-node-id user-string accessnode1
```

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {port | linkagg}	Enables or disables PPPoE-IA on a port or a link aggregate port.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
clear pppoe-ia statistics	Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAGlobalAccessNodeIDFormatType
alaPPPoEIAGlobalAccessNodeIDStringValue
```

pppoe-ia circuit-id

Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop that receives the PPPoE Active Discovery Initiation (PADI) or PPPoE Active Discovery Request (PADR) or PPPoE Active Discovery Terminate (PADT) from the user end.

pppoe-ia circuit-id {default [atm] ascii [base-mac | system-name | interface | vlan | cvlan | interface-alias | user-string *string* **| delimiter** *char***]}**

Syntax Definitions

default	The default value of the Circuit-ID used for the Ethernet parameter.
atm	When the PPPoE-IA Circuit-ID format is configured as “default atm” the Circuit-ID encoding happens for “ATM” (Asynchronous Transfer Mode) parameter.
ascii	Circuit-ID format used to configure Circuit-ID string using the five parameters and delimiter. Maximum five parameters can be selected from the given seven options: base-mac, system-name, interface, vlan, cvlan, interface-alias, and user-string.
base-mac	The base MAC address of the switch.
system-name	Name configured for the switch.
interface	The interface on which the PPPoE message is received.
vlan	VLAN interface on which the PPPoE message is received.
cvlan	Inner-VLAN or customer VLAN of the PPPoE message.
interface-alias	Configured alias of the interface on which the PPPoE message is received.
string	The value of user configured string.
delimiter	A user configurable delimiter used to separate the fields of an ASCII string forming the Circuit-ID.
char	The value (a character) of the user configurable delimiter.

Defaults

parameter	default
char	**:**

By default, “:” (colon) is used as the delimiter.

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

- Circuit-ID identification is configurable only globally and cannot be configured on a per-port or per-VLAN basis.

- To configure ethernet default parameter, use “default” in the CLI command.
- To configure default parameter as “atm”, use “default ATM” in the CLI command.
- When the PPPoE-IA Circuit-ID format is configured as “default atm” the Circuit-ID encoding happens for “ATM” (Asynchronous Transfer Mode) parameter.
- By default, the value of the Circuit-ID is "access-node-id eth slot/port[:vlan-id]". For example, if the value of access-node-id is "vxTarget", the default value of Circuit-ID is "vxTarget eth 1/1:10", if the packet is received on the interface 1/1 in vlan 10.
- By default, the delimiter used is “:”. The available delimiters are: “:” (colon), “|” (pipe), “/” (forward slash), “\” (backward slash), “-” (hyphen), “'_” (underscore), “ ” (space), “#” (hash), “.” (full stop), “,” (comma), “;” (semicolon).
- The Circuit-ID can have a maximum of 63 characters. The Circuit-ID longer than 63 characters is truncated to 63 characters.
- At most, five fields out of the available seven is encoded for the Circuit-ID in the order specified by the user.
- If the access-node-identifier is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.
- The value of user string must not be NULL.
- You can configure the same Circuit-ID format multiple times (for example, base MAC address of the switch can be configured multiple times in ASCII format of Circuit-ID).
- If the Circuit-ID format is default, irrespective of the ASCII fields (if configured), the Circuit-ID configuration is not visible in **show pppoe-ia configuration** output.

Examples

```
-> pppoe-ia circuit-id default
-> pppoe-ia circuit-id default atm
-> pppoe-ia circuit-id ascii base-mac vlan
-> pppoe-ia circuit-id ascii system-name interface user-string cid1
-> pppoe-ia circuit-id ascii system-name delimiter #
```

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAGlobalCircuitIDFormatType
alaPPPoEIAGlobalCircuitIDField1
alaPPPoEIAGlobalCircuitIDField1StrVal
alaPPPoEIAGlobalCircuitIDField2
alaPPPoEIAGlobalCircuitIDField2StrVal
alaPPPoEIAGlobalCircuitIDField3
alaPPPoEIAGlobalCircuitIDField3StrVal
alaPPPoEIAGlobalCircuitIDField4
alaPPPoEIAGlobalCircuitIDField4StrVal
alaPPPoEIAGlobalCircuitIDField5
alaPPPoEIAGlobalCircuitIDField5StrVal
alaPPPoEIAGlobalCircuitIDDelimiter
```

pppoe-ia remote-id

Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.

pppoe-ia remote-id {base-mac | system-name | mgnt-address | user-string *string***}**

Syntax Definitions

base-mac	The base MAC address of the switch.
system-name	The name configured for the switch.
mgnt-address	The management IP address of the switch.
string	The value configured for user string.

Defaults

By default, the base MAC address of the switch is used as the format for Remote-ID.

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

- Remote-ID is configurable only globally and cannot be configured on a per-port or per-VLAN basis.
- Remote-ID can have a maximum of 63 characters. The Remote-ID longer than 63 characters is truncated to 63 characters.
- In case of management address format, IP address of the Loopback0 interface (if configured and active) or the first active IP interface address is used as the management address. If none of them are available, IP address ‘0.0.0.0’ is used as management address.
- If the Remote-ID is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.
- The value of user string must not be NULL.

Examples

```
-> pppoe-ia remote-id base-mac
-> pppoe-ia remote-id user-string remoteuser1
```

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAGlobalRemoteIDFormatType
alaPPPoEIAGlobalRemoteIDStringValue
```

clear pppoe-ia statistics

Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.

clear pppoe-ia statistics [port {*chassis/slot/port*[*-port2*] **| linkagg** *agg_num***]**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for the module.
port	Port number of the interface to be configured.
port2	Last port number in a range of ports to be configured.
linkagg *agg_num*	Specifies the link aggregate identification number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

N/A

Examples

```
-> clear pppoe-ia statistics
-> clear pppoe-ia statistics linkagg 13
```

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia access-node-id	Globally configures a format to form an identifier that uniquely identifies an access node.
pppoe-ia circuit-id	Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAGlobalClearStats
alaPPPoEIAStatsTable
   alaPPPoEIAStatsClearStats
```

show pppoe-ia configuration

Displays the global configuration for PPPoE-IA.

show pppoe-ia configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

- If the Circuit-ID is configured with “default” parameter, then the Circuit-ID format will display as “ethernet”.
- If the Circuit-ID is configured with “default atm” parameter, then the Circuit-ID format will display as “atm”.

Examples

```
Default Configuration
-> pppoe-ia circuit-id default
-> show pppoe-ia configuration
Status                     : disabled,
Access Node Identifier
  Access-node-id Format    : base-mac,
  Access-node-id String    : 00:d0:95:ee:fb:02,
Circuit Identifier
  Circuit-Id Format        : ethernet,
  Circuit-id Field1        : none,
  Circuit-id Field1 String : ,
  Circuit-id Field2        : none,
  Circuit-id Field2 String : ,
  Circuit-id Field3        : none,
  Circuit-id Field3 String : ,
  Circuit-id Field4        : none,
  Circuit-id Field4 String : ,
  Circuit-id Field5        : none,
  Circuit-id Field5 String : ,
  Circuit-id Delimiter     : ":",
Remote Identifier
  Remote-id Format         : base-mac,
  Remote-id String         : 00:d0:95:ee:fb:02
```

```
-> pppoe-ia circuit-id default atm
-> show pppoe-ia configuration
Status                     : enabled,
Access Node Identifier
  Access-node-id Format    : base-mac,
  Access-node-id String    : 00:d0:95:ee:fb:02,
Circuit Identifier
  Circuit-Id Format        : atm,
  Circuit-id Field1        : none,
  Circuit-id Field1 String : ,
  Circuit-id Field2        : none,
  Circuit-id Field2 String : ,
  Circuit-id Field3        : none,
  Circuit-id Field3 String : ,
  Circuit-id Field4        : none,
  Circuit-id Field4 String : ,
  Circuit-id Field5        : none,
  Circuit-id Field5 String : ,
  Circuit-id Delimiter     : ":",
Remote Identifier
  Remote-id Format         : base-mac,
  Remote-id String         : 00:d0:95:ee:fb:02
```

output definitions

Status	Displays the global PPPoE-IA status: Enabled or Disabled.
Access-node-id Format	The format used to form an identifier that uniquely identifies an access node.
Access-node-id String	The value of user configured string for the access node.
Circuit-Id Format	The format used to form an identifier that uniquely identifies an access node and an access loop.
Circuit-id Field1	The Circuit-ID format.
Circuit-id Field1 String	The value of Circuit-ID depending on the format configured for the Circuit-ID.
Circuit-id Delimiter	A user configurable delimiter (a character) used to separate the fields of an ASCII string forming the Circuit-ID.
Remote-id Format	The format used to form an identifier that uniquely identifies the user attached to the access loop.
Remote-id String	The value of user configured string for the Remote-ID.

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia access-node-id	Globally configures a format to form an identifier that uniquely identifies an access node.
pppoe-ia circuit-id	Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.
pppoe-ia remote-id	Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAGlobalStatus
   alaPPPoEIAGlobalAccessNodeIDFormatType
   alaPPPoEIAGlobalAccessNodeIDStringValue
   alaPPPoEIAGlobalCircuitIDFormatType
   alaPPPoEIAGlobalCircuitIDField1
   alaPPPoEIAGlobalCircuitIDField1StrVal
   alaPPPoEIAGlobalCircuitIDField2
   alaPPPoEIAGlobalCircuitIDField2StrVal
   alaPPPoEIAGlobalCircuitIDField3
   alaPPPoEIAGlobalCircuitIDField3StrVal
   alaPPPoEIAGlobalCircuitIDField4
   alaPPPoEIAGlobalCircuitIDField4StrVal
   alaPPPoEIAGlobalCircuitIDField5
   alaPPPoEIAGlobalCircuitIDField5StrVal
   alaPPPoEIAGlobalCircuitIDDelimiter
   alaPPPoEIAGlobalRemoteIDFormatType
   alaPPPoEIAGlobalRemoteIDStringValue
   alaPPPoEIAGlobalClearStats
```

show pppoe-ia {port | linkagg}

Displays the following:

- PPPoE-IA configuration for a physical or link-aggregate port, physical port range, or all the physical or link-aggregate ports.
- Port or port range configuration for ports with PPPoE-IA enabled or disabled
- Ports that are configured as trust or client port for PPPoE-IA.

show pppoe-ia {port {*chassis/lot/port*[*-port2*] **| linkagg** *agg_num***} [enabled | disabled | trusted | client]**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for the module.
port	Port number of the interface to be configured.
port2	Last port number in a range of ports to be configured.
linkagg *agg_num*	Specifies the link aggregate identification number.
enabled	PPPoE-IA enabled port.
disable	PPPoE-IA disabled port.
trust	Port configured as trust.
client	Port configured as client.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

N/A

Examples

```
Default Configuration
-> show pppoe-ia port
Chassis/
Slot/Port    Status      Mode
----------+----------+------------
1/1/1        enabled     client
1/1/2        disabled    trusted
1/1/3        disabled    client
1/1/4        enabled     trusted
.
.
1/1/24        enabled     client
```

```
0/0         enabled     client
0/1         disabled    trusted

-> show pppoe-ia linkagg 1 enabled
ERROR: PPPoE-IA is disabled on linkagg 1

-> show pppoe-ia port 1/1/1 trusted
Chassis/Slot/Port   Status
----------+----------
1/1/1        enabled

-> show pppoe-ia port 1/1/1-5 client
Chassis/Slot/Port   Status
----------+----------
1/1/1        enabled
1/1/2        disabled
1/1/5        disabled
```

output definitions

Chassis/Slot/Port	Chassis, slot and port number.
Status	PPPoE-IA enabled or disabled port.
Mode	Port configured as trust or client port for PPPoE-IA.

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
clear pppoe-ia statistics	Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia statistics	Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

```
alaPPPoEIAGlobalStatus
alaPPPoEIAGlobalAccessNodeIDFormatType
alaPPPoEIAGlobalAccessNodeIDStringValue
alaPPPoEIAGlobalCircuitIDFormatType
alaPPPoEIAGlobalCircuitIDField1
alaPPPoEIAGlobalCircuitIDField1StrVal
alaPPPoEIAGlobalCircuitIDField2
alaPPPoEIAGlobalCircuitIDField2StrVal
alaPPPoEIAGlobalCircuitIDField3
alaPPPoEIAGlobalCircuitIDField3StrVal
alaPPPoEIAGlobalCircuitIDField4
alaPPPoEIAGlobalCircuitIDField4StrVal
alaPPPoEIAGlobalCircuitIDField5
alaPPPoEIAGlobalCircuitIDField5StrVal
alaPPPoEIAGlobalCircuitIDDelimiter
alaPPPoEIAGlobalRemoteIDFormatType
alaPPPoEIAGlobalRemoteIDStringValue
```

show pppoe-ia statistics

Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

show pppoe-ia {port {*chassis/slot/port*[*-port2*] **| linkagg** *agg_num***} statistics**

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number for the module.
port	Port number of the interface to be configured.
port2	Last port number in a range of ports to be configured.
linkagg *agg_num*	Specifies the link aggregate identification number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6865

Usage Guidelines

N/A

Examples

```
Default Configuration
-> show pppoe-ia statistics
Chassis/
Slot/  PADI   PADR   PADT    PADI     PADR    PADT    PADO    PADS
Port    Rx     Rx     Rx    Discard  Discard Discard Discard Discard
------+------+------+------+--------+-------+-------+-------+--------
1/1/1     2      2      0      1        0       0       2       3
1/1/2     2      1      0      1        0       0       2       0
1/1/3     3      2      2      2        1       2       2       3
.
.
1/1/24    2      2      0      1        0       0       2       3
0/0     2      2      0      1        0       0       2       3
0/1     2      2      0      1        0       0       2       3

-> show pppoe-ia linkagg 1 statistics
Slot/  PADI   PADR   PADT    PADI     PADR    PADT    PADO    PADS
Port    Rx     Rx     Rx    Discard  Discard Discard Discard Discard
------+------+------+------+--------+-------+-------+-------+--------
0/1     2      2      0      1        0       0       2       3
```

output definitions

Chassis/Slot/Port	Chassis, slot and port number.
PADI Rx	Valid PADI (PPPoE Active Discovery Initiation) packets received on the client port.
PADR Rx	Valid PADR (PPPoE Active Discovery Request) packets received on the client port.
PADT Rx	Valid PADT (PPPoE Active Discovery Terminate) packets received on the client port.
PADI Discard	Invalid (malformed or PDU length exceeds 1484) PADI packets received on the client port or no enabled trust port in the same VLAN as the client port.
PADR Discard	Invalid (malformed or PDU length exceeds 1500) PADR packets received on client port or no enabled trust port in the same VLAN as the client port.
PADT Discard	Invalid (malformed or PDU length exceeds 1500) PADT packets received on client port or no enabled trust port in the same VLAN as the client port.
PADO Discard	Total PADO (PPPoE Active Discovery Offer) packets received on the client port.
PADS Discard	Total PADS (PPPoE Active Discovery Session-confirmation) packets received on the client port.

Release History

Release 8.6R1; command introduced.

Related Commands

pppoe-ia access-node-id	Globally configures a format to form an identifier that uniquely identifies an access node.
pppoe-ia circuit-id	Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.
pppoe-ia remote-id	Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.
clear pppoe-ia statistics	Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.

MIB Objects

```
alaPPPoEIAStatsTable
   alaPPPoEIAStatsIfIndex
   alaPPPoEIAStatsPADIRxCounter
   alaPPPoEIAStatsPADRRxCounter
   alaPPPoEIAStatsPADTRxCounter
   alaPPPoEIAStatsPADIRxDiscardCounter
   alaPPPoEIAStatsPADRRxDiscardCounter
   alaPPPoEIAStatsPADTRxDiscardCounter
   alaPPPoEIAStatsPADORxDiscardCounter
   alaPPPoEIAStatsPADSRxDiscardCounter
```

56 Service Assurance Agent Commands

Service Assurance Agent (SAA) enables customers to assure new business-critical applications, as well as services that utilize data, voice, and video. Use SAAs to verify service guarantees, increase network reliability by validating network performance, proactively identify network issues, and increase return on investment (ROI) by easing the deployment of new services. The SAA feature uses active monitoring to generate traffic in a continuous, reliable, and predictable manner, thus enabling the measurement of network performance and health.

IP SAAs enhance the service level monitoring to become IP application-aware by measuring both end-to-end and at the IP layer. IP SAA would allow performance measurement against any IP addresses in the network (switch, server, pc). Use ETH-LB/DMM to measure delay and jitter by sending out frames with DM information to the peer MEP and receiving frames with DM information from the peer MEP.

MIB information for the SAA commands is as follows:

Filename: Alcatel-IND1-ETHERNET-OAM-MIB.mib
Module: alcatelIND1EoamMIB

Filename: IEEE8021-CFM-MIB.mib
Module: ieee8021CfmMib

Filename: ALCATEL-IND1-SAA-MIB.mib
Module: alcatelIND1SaaMIB

A summary of the available commands is listed here:

SAA Commands	**saa** **saa start** **saa stop**
EthOAM SAA Commands	**saa type ethoam-loopback** **saa type ethoam-two-way-delay**
IP SAA Command	**saa type ip-ping**
Layer 2 SAA Command	**saa type mac-ping**
SPB SAA Commands	**saa spb** **saa spb reset** **saa spb flush** **show saa spb**
XML SAA Commands	**saa xml** **show saa xml**
SAA Show Commands	**show saa** **show saa type config** **show saa statistics**

saa

Configures a Service Assurance Agent (SAA).

saa *string* **[descr** *description***] [interval** *interval***] [jitter-threshold** *jitter_thresh***] [rtt-threshold** *rtt_thresh***]**

no saa *string*

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if SAA ID contains multiple words with spaces between them (for example “SAA 10”).
description	Text string up to 32 characters. Use quotes around string if description contains multiple words with spaces between them (for example, “ALE Marketing SAA”).
interval	The amount of time, in minutes, between two iterations of the SAA test. Valid range is from 1, 2, 5, 10 to 1500.
jitter_thresh	The jitter threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.
rtt_thresh	The round-trip time threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.

Defaults

parameter	default
description	DEFAULT
interval	150 minutes
jitter_thresh	0 (disabled)
rtt_thresh	0 (disabled)

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove an SAA from the switch configuration. Note that the SAA must be stopped before it can be deleted.
- The **desc** and **interval** parameters are optional. If these values are specified, the SAA is created with those values. If these values are not specified, the SAA is created with the default values.
- If the **desc** and/or **interval** parameters are specified for an existing SAA, then the values of the existing parameters are updated with those specified.
- If the session time interval is changed for an SAA that is already running and active, the interval value is immediately updated in the database but is not applied to the SAA until after the next iteration.

- If none of the optional parameters are specified and the given SAA exists, the CLI will return an error message, as duplicate entries are not allowed.
- Any number of SAAs can be configured (MAX 127). It is recommended not to start many aggressive SAAs (having session interval <= 10). To achieve proper scheduling of all the started SAA (aggressive and relaxed) it is recommended not to start more than 50 SAAs.
- Ensure the interval value is greater than the execution time (number of packets * inter packet delay).
- When SAA processes an iteration of a session, it will compare the results against the following criteria to see if an SNMP trap should be sent. A trap with the session name is sent if:
  - At least one packet is lost.
  - Warning: Average RTT/Jitter crosses 90% of threshold.
  - Critical: Average RTT/Jitter at or above threshold.

Examples

```
-> saa saa1 descr “saa for ip-ping”
-> saa saa1 jitter-threshold 100 rtt-threshold 500
-> saa saa2 descr “Monitoring Default VRF-interface” interval 160
-> saa saa2 interval 120
-> no saa saa1
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.2; **jitter-threshold** and **rtt-threshold** parameters added.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlRowStatus
   alaSaaCtrlDescr
   alaSaaCtrlInterval
   alaSaaCtrlJitterThreshold
   alaSaaCtrlRTTThreshold
```

saa type ip-ping

Configure SAA for IP including the number of packets and inter-packet delay parameters.

saa *string* **type ip-ping destination-ip** *ip_address* **source-ip** *ip_address* **type-of-service** *tos* **[num-pkts** *count***] [inter-pkt-delay** *delay***] [payload-size** *size***]**

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if the SAA ID contains multiple words with spaces between them (for example, “SAA 10”).
destination-ip *ip_address*	The IPv4 address of the destination to ping.
source-ip *ip_address*	The IPv4 address of the source.
tos	The type of service. Valid range is 0 – 255.
count	The number of packets to send in one ping iteration. The valid range is 1–100.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is from 100 ms to 1000 ms in multiples of 100 ms.
size	The size of the ICMP payload to be used for the ping iteration. Valid range is 24–1472 bytes.

Defaults

parameter	default
count	5
delay	1000 ms
size	24 bytes

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The **num-pkts**, **inter-pkt-delay,** and **payload-size** are optional parameters. If these values are specified, the SAA is created with the values entered. If none of them are specified, the SAA is created with the default values. The **num-pkts** and **inter-pkt-delay** can be modified, but **payload-size** cannot be modified later.
- Total execution time, that is, the product of **num-pkts** and **inter-pkt-delay (**number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.
- The SAA must not be in a ‘started’ state at the time the **num-pkts** or **inter-pkt-delay** parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return an error.

- Do not specify a broadcast or multicast address for the source or destination IP. In addition, do not use 0.0.0.0 as the destination IP address.
- The timeout for each ping request packet is 1 sec. This value is not configurable.

Examples

```
-> saa saa1 type ip-ping destination-ip 123.32.45.76 source-ip 123.35.42.124 type-
of-service 4
-> saa saa2 type ip-ping destination-ip 123.32.45.77 source-ip 123.35.42.124 type-
of-service 5
-> saa saa3 type ip-ping destination-ip 123.32.55.27 source-ip 123.35.42.125 type-
of-service 8 inter-pkt-delay 1000
-> saa saa4 type ip-ping destination-ip 123.46.45.77 source-ip 123.35.42.125 type-
of-service 2 num-pkts 5
-> saa saa5 type ip-ping destination-ip 12.53.45.77 source-ip 123.35.42.125 type-
of-service 35 payload-size 1000
-> saa saa6 type ip-ping destination-ip 123.22.45.66 source-ip 123.35.42.125 type-
of-service 5 inter-pkt-delay 1000 num-pkts 8 pkt-size 1000
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaIpCtrlTable
   alaSaaIpCtrlTestIndex
   alaSaaIpCtrlRowStatus
   alaSaaIpCtrlTestMode
   alaSaaIpCtrlTgtAddress
   alaSaaIpCtrlSrcAddress
   alaSaaIpCtrlTypeOfService
   alaSaaIpCtrlInterPktDelay
   alaSaaIpCtrlPayloadSize
   alaSaaIpCtrlNumPkts
```

saa type mac-ping

Configure SAA for a MAC address including the VLAN, VLAN ID, number of packets and inter-packet delay parameters.

saa *string* **type mac-ping destination-mac** *mac_address* **vlan** *vlan_id* **[vlan-priority** *vlan_priority***] [drop-eligible {true | false}] [data** *data***] [num-pkts** *count***] [inter-pkt-delay** *delay***] [payload-size** *size***] [isid-check** *isid***]**

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if the SAA ID contains multiple words with spaces between them (for example, “SAA 10”).
mac_address	The destination MAC address to ping.
vlan_id	The VLAN on which the L2 SAA Packets will be sent out.Valid range is 1-4094.
vlan_priority	Specifies both the internal priority of the MAC ping and the 802.1p value on the VLAN tag header. Valid range is 0-7.
true	Sets both the internal drop precedence of the MAC ping and the CFI bit on the VLAN tag header to true.
false	Sets both the internal drop precedence of the MAC ping and the CFI bit on the VLAN tag header to false.
data	User specified string to be included in the packet (Data TLV).
count	The number of packets to send in one ping iteration.The valid range is 1–100.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is from 100 ms to 1000 ms in multiples of 100 ms.
size	The size of the ICMP payload to be used for the ping iteration. Valid range is 36–1500 bytes.
isid	A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network.

Defaults

parameter	default
vlan_priority	0
true | **false**	false
count	5
delay	1000 ms
size	36 bytes

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The **num-pkts**, **inter-pkt-delay**, and **payload-size** are optional parameters. If these values are specified, the SAA is created with the values entered. If none of them are specified, the SAA is created with the default values. The **num-pkts** and **inter-pkt-delay** can be modified, but **payload-size** cannot be modified later.
- Total execution time, that is, the product of **num-pkts** and **inter-pkt-delay (**number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.
- The SAA must not be in a 'started' state at the time the **num-pkts** or **inter-pkt-delay** parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return an error.
- The timeout for each ping request packet is 1 sec. This value is not configurable.
- If data-TLV is specified and payload size is not specified, then payload size will be increased internally to accommodate the data TLV.
- If data TLV and payload size both are specified and payload size is less than [dataTLV + 36] bytes (for time-stamping and other packet info), then the CLI will be rejected.
- Destination-MAC cannot be broadcast/multicast address.
- Timeout for each ping request packet is 1 sec. This value is non-configurable.

Examples

```
-> saa saa1 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10
-> saa saa4 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10 inter-pkt-delay
100
-> saa saa5 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10 num-pkts 10
-> saa saa6 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10 payload-size
400
-> saa saa8 type mac-ping destination-mac 00:11:11:11:11:11 vlan 1001 isid-check
1002
```

Release History

Release 7.3.1; command was introduced.
Release 8.6R1; **vlan-priority** and **drop-eligible** parameters deprecated.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaMacCtrlTable
   alaSaaMacCtrlDstAddress
   alaSaaMacCtrlVlan
   alaSaaMacCtrlVlanPriority
   alaSaaMacCtrlPktData
   alaSaaMacCtrlDropEligible
   alaSaaMacCtrlPayloadSize
   alaSaaMacCtrlNumPkts
   alaSaaMacCtrlInterPktDelay
   alaSaaMacCtrlIsid
```

saa spb

Configures session parameters for the Shortest Path Bridging (SPB) SAA. The SPB feature dynamically discovers SPB-enabled switches. Each discovered switch is identified by the pairing of a SPB VLAN (BVLAN) and the backbone MAC address (BMAC) for the switch. SPB advertises these BVLAN-BMAC pairs to the SAA feature, which in turn creates and starts MAC ping sessions based on the parameters configured with this command.

saa spb [auto-create] [auto-start] [interval *interval***] [vlan-priority** *vlan_priority***] [drop-eligible** {**true** | **false**}**] [data** *data***] [num-pkts** *count***] [inter-pkt-delay** *delay***] [payload-size** *size***] [jitter-threshold** *jitter_thresh***] [rtt-thresh** *rtt_thresh***] [keep]**

Syntax Definitions

auto-create	Automatically creates a SPB SAA session for each discovered BVLAN-BMAC pair.
auto-start	Automatically starts each SPB SAA session.
interval	The amount of time, in minutes, between two iterations of the SAA test. Valid range is from 1, 2, 5, 10–1500.
vlan_priority	Specifies both the internal priority of the MAC ping and the 802.1p value on the VLAN tag header. Valid range is 0-7.
true	Sets both the internal drop precedence of the MAC ping and the CFI bit on the VLAN tag header to true.
false	Sets both the internal drop precedence of the MAC ping and the CFI bit on the VLAN tag header to false.
data	User specified string to be included in the packet (Data TLV).
count	The number of packets to send in one ping iteration of the test.Valid range is 1–100.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is 100–1000 ms in multiples of 100 ms.
size	The size of the ICMP payload to be used for the ping iteration. Valid range is 32–1500 bytes.
jitter_thresh	The jitter threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.
rtt_thresh	The round-trip time threshold value, in microseconds. A trap is generate when this value is crossed. The valid range is 0–1000000.
keep	Retains SPB SAA session information even when SPB signals that a BMAC or BVLAN no longer exists.

Defaults

parameter	default
auto-create	off
auto-start	off
interval	150 minutes
vlan-priority	0
drop-eligible {true | **false}**	false
data	null
count	5
delay	1000 ms
size	32 bytes
jitter_thresh	0 (disabled)
rtt-thresh	0 (disabled)
keep	off

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

- The **auto-create** and **auto-start** parameters enable the SPB SAA functionality required to automatically create and start this type of SAA session.
- Ensure the interval value is greater than the execution time (number of packets * inter-packet delay).
- Total execution time, that is, the product of **num-pkts** and **inter-pkt-delay (**number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.
- SPB SAA sessions cannot be modified but are automatically configured with “SPB” as the owner of the session so they can be easily identified within the applicable SAA **show** command displays.
- The SAA ID for an SPB SAA is the prefix SPB- combined with the BVLAN and BMAC pairing used to generate the session. For example, SPB-*bvlan-bmac* (SPB-4000-e8-e7-32-07-98-cd).

Examples

```
-> saa spb auto-create auto-start interval 160 num-pkts 50 inter-pkt-delay 100 keep
-> saa spb auto-create auto-start jitter-threshold 100 rtt-threshold 500
-> saa spb keep
```

Release History

Release 7.3.2; command was introduced.
Release 8.6R1; **vlan-priority** and **drop-eligible** parameters deprecated.

Related Commands

show saa spb	Displays the SAA configuration for the SPB SAA.
saa spb flush	Clears all SPB SAA sessions and rebuilds the sessions based on the information learned from SPB.
saa spb reset	Resets all SPB SAA session parameters back to their default values.

MIB Objects

```
alaSaaSpbFeature
   alaSaaSpbAutoCreate
   alaSaaSpbAutoStart
   alaSaaSpbInterval
   alaSaaSpbVlanPriority
   alaSaaSpbDropEligible
   alaSaaSpbPktData
   alaSaaSpbNumPkts
   alaSaaSpbInterPktDelay
   alaSaaSpbPayloadSize
   alaSaaSpbJitterThreshold
   alaSaaSpbRTTThreshold
   alaSaaSpbKeep
```

saa spb reset

Resets all of the SPB SAA session parameters to their default values.

saa spb reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

When this command is used, the SPB SAA session parameters are set to the following default values:

parameter	default
auto-create	off
auto-start	off
interval	150 minutes
vlan-priority	0
drop-eligible	false
data	null
count	5
delay	1000 ms
size	32 bytes
jitter_thresh	0 (disabled)
rtt-thresh	0 (disabled)
keep	off

Examples

```
-> saa spb reset
```

Release History

Release 7.3.2; command was introduced.
Release 8.6R1; **vlan-priority** and **drop-eligible** parameters deprecated.

Related Commands

show saa spb	Displays the SAA configuration for the SPB SAA.
saa spb flush	Clears all SPB SAA sessions and rebuilds the sessions based on the information learned from SPB.
saa spb	Configures SPB SAA session parameters.

MIB Objects

```
alaSaaSpbFeature
   alaSaaSpbReset
```

saa spb flush

Clears all SPB SAA sessions and rebuilds the sessions based on the information learned from SPB.

saa spb flush

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

This command does *not* stop the automatic creation or start of SPB sessions or change any of the SPB SAA session parameters.

Examples

```
-> saa spb flush
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show saa spb	Displays SAA configuration information.
saa spb reset	Resets all SPB SAA session parameters back to their default values.
saa spb	Configures SPB SAA session parameters.

MIB Objects

```
alaSaaSpbFeature
   alaSaaSpbReset
```

saa type ethoam-loopback

Configures the SAA for ETH-LB, including the number of packets and inter-packet delay parameters.

saa *string* **type ethoam-loopback {target-endpoint** *t_mepid* **| target-mac address** *mac_address***} source-endpoint** *s_mepid* **domain** *md_name* **association** *ma_name* **vlan-priority** *vlan_priority* **[drop-eligible {true | false}] [data** *data***] [num-pkts** *num***] [inter-pkt-delay** *delay***]**

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if the SAA ID contains multiple words with spaces between them (for example, “SAA 10”).
t_mepid	The ID of the destination MEP.
mac_address	The MAC address of the destination.
s_mepid	The ID of the source MEP.
md_name	The domain to which the source MEP belongs.
ma_name	The association to which the source MEP belongs.
vlan_priority	The VLAN priority to be used for the outgoing packet. The valid range is 0-7.
true	Sets the drop eligibility bit in the VLAN tag to true.
false	Sets the drop eligibility bit in the VLAN tag to false.
data	User specified string that is included in the packet.
num	The number of packets to send during loopback. Valid range is 1– 100.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is 100–1000 ms in multiples of 100 ms.

Defaults

parameter	default
drop-eligible {true | false}	false
num-pkts *num*	5
delay	1000

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return error.
- Source MEP-ID, MD and MA must be created before initiating loopback.
- If the source MEP-Id/MA/MD does not exist, the configuration will be accepted and no error will be returned.
- When **target-endpoint** is specified then it must be learned before initiating loopback.
- When **target-endpoint** is specified and learned, Ethernet Loopback will be transmitted irrespective of whether the RMEP state is OK or failed.
- The **data**, **num-pkts,** and **inter-pkt-delay** are optional parameters. If these values are specified, the entry will be created with these values. If none of them are specified, the SAA will be created with default values. The **num-pkts** and **inter-pkt-delay** can be modified later.
- Total execution time, that is, the product of **num-pkts** and **inter-pkt-delay (**number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.
- The SAA must not be in a ‘started’ state at the time the **num-pkts** or **inter-pkt-delay** parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- The Target MEP/MAC, source MEP, domain, and association parameters are mandatory. If they are not specified, the CLI will return an error.
- The **data** parameter is optional. If this parameter is not specified, then it is not sent in the loopback message.
- The timeout value for each LB packet is one second. This value is not configurable.

Examples

```
-> saa saa1 type ethoam-loopback target-endpoint 10 source endpoint 1 domain md1
association ma1
-> saa saa2 type ethoam-loopback target-endpoint 10 source endpoint 2 domain md1
association ma1 data « monitor association ma1 » num-pkts 6 inter-pkt-delay 500
-> saa saa3 type ethoam-loopback target-endpoint 15 source endpoint 1 domain md1
association ma1 data « monitor association ma1 » num-pkts 6
-> saa saa4 type ethoam-loopback target-endpoint 10 source endpoint 2 domain md1
association ma1 inter-pkt-delay 500
```

Release History

Release 7.3.1; command was introduced.
Release 8.6R1; **vlan-priority** and **drop-eligible** parameters deprecated.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaEthoamCtrlTable
   alaSaaEthoamCtrlTestIndex
   alaSaaEthoamCtrlRowStatus
   alaSaaEthoamCtrlTestMode
   alaSaaEthoamCtrlTgtMAC
   alaSaaEthoamCtrlSrcMepId
   alaSaaEthoamCtrlDomainName
   alaSaaEthoamCtrlAssociationName
   alaSaaEthoamCtrlNumPkts
   alaSaaEthoamCtrlInterPktDelay
   alaSaaEthoamCtrlPktData
   alaSaaEthoamCtrlVlanPriority
```

saa type ethoam-two-way-delay

Configures SAA for ETH-DMM, including the number of packets and inter-packet delay parameters.

saa *string* **type {ethoam-two-way-delay} {target-endpoint** *t_mepid* **| target-mac address** *mac_address***} source-endpoint** *s_mepid* **domain** *md_name* **association** *ma_name* **vlan-priority** *vlan_priority* **[num-pkts** *num***] [inter-pkt-delay** *delay***]**

Syntax Definitions

string	SAA ID string up to 32 characters. Use quotes around string if the SAA ID contains multiple words with spaces between them (for example, “SAA 10”).
t_mepid	The ID of the destination MEP.
mac_address	The MAC address of the destination.
s_mepid	The ID of the source MEP.
md_name	The domain to which the source MEP belongs.
ma_name	The association to which the source MEP belongs.
vlan_priority	The VLAN priority to be used for the outgoing packet. The valid range is 0-7.
num	The number of packets to send during loopback. Valid range is 1– 100.
delay	The delay between packets sent during a ping iteration, in milliseconds. Valid range is 100–1000 ms in multiples of 100 ms.

Defaults

parameter	default
num	5
delay	1000

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- The SAA should exist before issuing the CLI. If the SAA does not exist, the CLI will return error.
- The source MEP-ID, MD, and MA must be created before initiating DMM.
- If the source MEP-Id/MA/MD does not exist, the configuration will be accepted and no error will be returned.
- When the **target-endpoint** parameter is specified, then it must be learned before initiating DMM.
- When the **target-endpoint** parameter is specified and learned, ETH-DMM will be transmitted irrespective of whether the RMEP state is OK or failed.

- The **num-pkts** and **inter-pkt-delay** parameters are optional. If these values are specified, the entry will be created with those values. If none of them are specified, the SAA will be created with default values. The **num-pkts** and **inter-pkt-delay** values can be modified, but the **pkt-size** value cannot be modified later.
- Total execution time, that is, the product of **num-pkts** and **inter-pkt-delay (**number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.
- The SAA must not be in a 'started' state at the time the **num-pkts** or **inter-pkt-delay** parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- Target MEP/MAC, source MEP, domain, and association parameters are mandatory. If they are not specified, the CLI will return an error.
- The timeout for each DMM packet is 1 sec. This value is not configurable.

Examples

```
-> saa saa1 type ethoam-two-way-delay target-endpoint 10 source endpoint 1 domain
md1 association ma1
-> saa saa2 type ethoam-two-way-delay target-endpoint 10 source endpoint 2 domain
md1 association ma1 num-pkts 6 inter-pkt-delay 500
-> saa saa3 type ethoam-two-way-delay target-endpoint 15 source endpoint 1 domain
md1 association ma1 num-pkts 6
-> saa saa4 type ethoam-two-way-delay target-endpoint 10 source endpoint 2 domain
md1 association ma1 inter-pkt-delay 500
```

Release History

Release 7.3.1; command was introduced.
Release 8.6R1; **vlan-priority** parameter deprecated.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaEthoamCtrlTable
   alaSaaEthoamCtrlTestIndex
   alaSaaEthoamCtrlRowStatus
   alaSaaEthoamCtrlTestMode
   alaSaaEthoamCtrlTgtMAC
   alaSaaEthoamCtrlSrcMepId
   alaSaaEthoamCtrlDomainName
   alaSaaEthoamCtrlAssociationName
   alaSaaEthoamCtrlNumPkts
   alaSaaEthoamCtrlInterPktDelay
   alaSaaEthoamCtrlVlanPriority
```

saa start

Starts the SAA test.

saa *string* **start [at** *yyyy-mm-dd,hh:mm:ss.ds***]**

Syntax Definitions

string	An existing SAA ID string.
yyyy-mm-dd,hh:mm:ss.ds	The date and time to start the SAA.

Defaults

By default, the SAA test is started immediately.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- An existing SAA with the SAA type configured must be specified with this command.
- Use the **saa stop** command to stop an SAA test that is already running.
- Use the **at** option to specify a date and time for the test to start.
- If an SAA is scheduled to start at a specified time and another **saa start** command with a different value is given before the specified time, the subsequent command will over-ride the previous command.
- If the **saa start** command is given after an SAA is started, then the CLI will return error.
- If the SAA type is configured with a source IP that does not exist or is not active, then the packet will not be transmitted and no error will be returned. Swlogs will be updated.
- ICMP must be enabled on the switch. If ICMP is disabled and an SAA of type ‘ip-ping’ is started, then the iteration will timeout and will be treated as failed iteration.
- Immediately after a CMM restart (reboot or takeover), the command to start SAA will be accepted, but the actual execution of the iteration will start 5 minutes after the CMM restart.
- If the SAA type is configured with a source MEP that does not exist or is not active (admin down), then the packet will not be transmitted and no error will be returned on the CLI console. Swlogs will be updated.
- It is recommended that all the SAAs be rescheduled if the system time is being changed.

Examples

```
-> saa saa2 start at 2009-09-12,09:00:00
-> saa saa4 start
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlStartAt
```

saa stop

Stops the SAA test.

saa *string* **stop [never | at** *yyyy-mm-dd,hh:mm:ss.d*s**]**

Syntax Definitions

string	An existing SAA ID string.
never	Specifies that the SAA test will not be stopped unless the **saa stop** command is used with the **at** option.
yyyy-mm-dd,hh:mm:ss.ds	The date and time to start the SAA.

Defaults

By default, the test is stopped immediately.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- An existing SAA with the SAA type configured must be specified with this command.
- The SAA must be in a ‘started’ state before giving the command unless the start and stop times are scheduled. If the SAA is not in a ‘started’ state, the CLI will return an error.
- Use the **at** option to specify a date and time for the test to stop.
- If the **never** option is specified, the SAA test will keep on running until the **saa stop** command is entered again with the **at** option.
- If SAA test is stopped while it is running an iteration, the current iteration is pre-empted. The statistics and history are updated for the partial iteration run.
- If an SAA is scheduled to stop at a specified time and another **saa stop** command with a different value is given before the specified time, the subsequent command will over-ride the previous command.

Examples

```
-> saa saa1 stop
-> saa saa2 stop never
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlStopAt
```

saa xml

Configures SAA XML parameters that determine when and where an SAA XML history file is created.

saa xml [file-name *xml_filename* **[interval** *interval***] [admin-state {enable | disable}]**

Syntax Definitions

xml_filename	The name of the file where SAA history entries are stored. This file must reside in the **/flash/network** directory on the local switch.
interval	The amount of time, in minutes, between each generation of the XML history file. Valid range is from 1–15000.
enable	Enables XML history file generation.
disable	Disables XML history file generation.

Defaults

parameter	default
xml_filename	saa.xml
interval	20 minutes
admin-state {enable | disable}	Disabled

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- When this function is enabled, SAA will periodically generate an XML file containing the following entries:
  - SAA name and ID
  - Iteration number
  - Last run time
  - Reason
  - Packets sent/Received
  - RTT min/avg/max
  - Jitter min/avg/max
  - Subports

Examples

```
-> saa xml interval 60 admin-state enable
-> saa xml file-name switch1_saa.xml interval 120 admin-status enable
```

Release History

Release 7.3.2; command was introduced.

Related Commands

show saa xml	Displays the SAA XML file generation parameters.

MIB Objects

```
alaSaaXmlFeature
   alaSaaXmlStatus
   alaSaaXmlFilename
   alaSaaXmlInterval
```

show saa

Displays SAA session information.

show saa [*string* | {**descr** *description*}**] [owner** *saa_owner***]**

Syntax Definitions

string	An existing SAA ID.
description	An existing SAA description string.
saa_owner	The owner name associated with the SAA session.

Defaults

By default, information is displayed for all SAA sessions.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the *string* or **descr** *description* parameter to display information for a specific SAA.
- Use the **owner** *saa_owner* parameter to display only those sessions initiated by a specific owner. The owner of an SAA session is not user configurable, but identifies the entity that created the session.
- When an SAA is created, an owner name is assigned to the agent. This name is based on the Alcatel-Lucent Enterprise application that generated the SAA and is not configurable. For example:
  - CLI SAA owner name = “USER”
  - OmniVista owner name = “OV”
  - Shortest Path Bridging owner name = “SPB” (SAA ID is SPB-*bvlan-bmac*)

Examples

```
-> show saa
Legend: eth-lb  = ethoam-loopback
        eth-dmm = ethoam-two-way-delay
SAA                        Owner  Type  Status Interval Time of Last Run Last Run Description
                                            (min)                      Result
--------------------------+-----+--------+------+-----+--------------------+-------+--------
SPB-4000-e8-e7-32-07-98-cd  SPB  mac-ping started   1  2013-03-06,18:01:35.0 success DEFAULT
Saa20                       USER ip-ping  started 130  2013-01-15,09:31:53.0 success DEFAULT
Saa31                       USER ip-ping  started 180  2013-01-12,21:30:05.0 failed  DC1
Saa90                       USER eth-lb   stopped 150  NOT RUN          undetermined DC5
Saa95                       USER eth-lb   stopped 300  2013-01-6,11:31:53.0  success EthLB

-> show saa SPB-4000-e8-e7-32-07-98-cd owner spb
Legend: eth-lb  = ethoam-loopback
        eth-dmm = ethoam-two-way-delay
SAA                        Owner  Type  Status Interval Time of Last Run Last Run Description
                                            (min)                      Result
--------------------------+-----+--------+------+-----+--------------------+-------+--------
SPB-4000-e8-e7-32-07-98-cd  SPB  mac-ping started   1  2013-03-06,18:01:35.0 success DEFAULT
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.2; **owner** parameter and field added.

Related Commands

saa	Configures an SAA.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlOwnerIndex
   alaSaaCtrlTestIndex
   alaSaaCtrlDescr
   alaSaaCtrlInterval
   alaSaaCtrlTestMode
   alaSaaCtrlLastRunTime
   alaSaaCtrlLastRunResult
   alaSaaCtrlAdminStatus
```

show saa type config

Displays the SAA configuration for the specified SAA type.

show saa [*string***] type {mac-ping | ip-ping | ethoam-loopback | ethoam-two-way-delay} config**

Syntax Definitions

string	An existing SAA ID.
mac-ping	Displays MAC Ping SAAs.
ip-ping	Displays IP Ping SAAs.
ethoam-loopback	Displays ETH-LB SAAs.
ethoam-two-way-delay	Displays ETH-DMM SAAs.

Defaults

By default, all SAAs with the specified type are displayed.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the *string* parameter to display information for a specific SAA
- If the SAA ID string specified does not match the specified SAA type, the CLI will return an error.

Examples

```
-> show saa type ip-ping config
SAA : saa20
  SAA-type              : ip-ping,
  Status                : started,
  Start At              : -
  Stop At               : 2010-02-08,12:00:00.0
  Description           : datacenter1,
  Interval(minutes)     : 130,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms)    : 0,
  Source-IP             : 0.0.0.0,
  Destination-IP        : 172.21.161.65,
  Payload-Size (bytes)  : 24,
  Type-of-Service       : 0,
  Num-pkts              : 5,
  Inter-pkt-delay       : 1000
SAA : saa31
  SAA-type              : ip-ping,
  Status                : started,
  Start At              : -
  Stop At               : -
  Description           : datacenter8,
  Interval(minutes)     : 180,
```

```
  Jitter Threshold (ms) : 100,
  RTT Threshold (ms)    : 500,
  Source-IP             : 0.0.0.0,
  Destination-IP        : 172.21.161.65,
  Payload-Size (bytes)  : 24,
  Type-of-Service       : 0,
  Num-pkts              : 5,
  Inter-pkt-delay       : 1000

-> show saa type ethoam-loopback config
Legend: Destination Mep: - = SAA configured with target mac-address
        Destination MAC: - = SAA configured with target mep-id
SAA : saa90
  SAA-type              : ethoam-loopback,
  Status                : started,
  Description           : SAA for ethernet-loopback,
  Interval(minutes)     : 300,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms)    : 0,
  Target-MAC            : -,
  Target-Endpoint       : 5,
  Source-Endpoint       : 1,
  Domain                : ale,
  Association           : ma1,
  Num-pkts              : 7,
  Inter-pkt-delay       : 1000,
  Data                  : ""
SAA : saa99
  SAA-type              : ethoam-loopback,
  Status                : started,
  Description           : SAA for ethernet-loopback,
  Interval(minutes)     : 300,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms)    : 0,
  Target-MAC            : 00:d0:b2:12:3c:a5,
  Target-Endpoint       : -,
  Source-Endpoint       : 5,
  Domain                : ale
  Association           : ma2,
  Num-pkts              : 5,
  Inter-pkt-delay       : 500

-> show saa type ethoam-two-way-delay config
Legend: Destination Mep: - = SAA configured with target mac-address
        Destination MAC: - = SAA configured with target mep-id
SAA : saa100
  SAA-type              : ethoam-two-way-delay,
  Status                : stopped,
  Description           : SAA for ethernet-two-way-test,
  Interval(minutes)     : 200,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms)    : 0,
  Target-MAC            : 00:d0:b2:12:3c:a5,
  Target-Endpoint       : -,
  Source-Endpoint       : 4,
  Domain                : aricent
  Association           : ma1,
  Num-pkts              : 5,
  Inter-pkt-delay       : 500
```

```
SAA : saa110
  SAA-type              : ethoam-two-way-delay,
  Status                : started,
  Description           : SAA for ethernet-two-way-delay,
  Interval(minutes)     : 300,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms)    : 0,
  Target-MAC            : -,
  Target-Endpoint       : 5,
  Source-Endpoint       : 1,
  Domain                : aricent
  Association           : ma2,
  Num-pkts              : 7,
  Inter-pkt-delay       : 800
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.2; **Jitter Threshold** and **RTT Threshold** fields added.

Related Commands

saa type mac-ping	Configures a MAC ping SAA.
saa type ip-ping	Configures an IP ping SAA.
saa type ethoam-loopback	Configures an ETH-LB SAA.
saa type ethoam-two-way-delay	Configures an ETH-DMM SAA.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlDescr
   alaSaaCtrlInterval
   alaSaaCtrlTestMode
   alaSaaCtrlJitterThreshold
   alaSaaCtrlRTTThreshold
alaSaaMacCtrlTable
   alaSaaMacCtrlDstAddress
   alaSaaMacCtrlPayloadSize
   alaSaaMacCtrlInterPktDelay
   alaSaaMacCtrlNumPkts
alaSaaIpCtrlTable
   alaSaaIpCtrlTgtAddress
   alaSaaIpCtrlSrcAddress
   alaSaaIpCtrlPayloadSize
   alaSaaIpCtrlTypeOfService
   alaSaaIpCtrlInterPktDelay
   alaSaaIpCtrlNumPkts
alaSaaEthoamCtrlTable
   alaSaaEthoamCtrlTestMode
   alaSaaEthoamCtrlAdminStatus
   alaSaaEthoamCtrlTgtMepId
   alaSaaEthoamCtrlTgtMAC
   alaSaaEthoamCtrlSrcMepId
   alaSaaEthoamCtrlNumPkts
   alaSaaEthoamCtrlInterPktDelay
```

show saa spb

Displays the SAA configuration for the Shortest Path Bridging (SPB) SAA.

show saa spb

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 6900, 9900, except 6900-V72, 6900-C32

Usage Guidelines

This command displays the SAA parameters that are applied to SPB SAA sessions. Use the **show saa** command to get specific session status and information.

Examples

```
-> show saa spb

SPB creation parameters:
  Auto-create           : Disabled,
  Auto-start            : Disabled,
  Interval(minutes)     : 150,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms)    : 0,
  Payload-Size (bytes)  : 32,
  Num-pkts              : 5,
  Inter-pkt-delay       : 1000,
  Keep                  : Disabled,
  Data                  : ""
```

Release History

Release 7.3.2; command was introduced.
Release 8.6R1; **Drop Eligible** and **Vlan-priority** fields removed.

Related Commands

saa spb	Configures a SPB SAA.
saa spb reset	Resets SPB SAA parameters to their default values.
saa spb flush	Clears SPB SAA sessions and rebuilds the sessions based on learned SPB information.

MIB Objects

```
alaSaaSpbFeature
   alaSaaSpbAutoCreate
   alaSaaSpbAutoStart
   alaSaaSpbInterval
   alaSaaSpbVlanPriority
   alaSaaSpbDropEligible
   alaSaaSpbPktData
   alaSaaSpbNumPkts
   alaSaaSpbInterPktDelay
   alaSaaSpbPayloadSize
   alaSaaSpbJitterThreshold
   alaSaaSpbRTTThreshold
   alaSaaSpbKeep
```

show saa xml

Displays the SAA XML file generation parameter configuration.

show saa xml

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show saa xml

XML file creation parameters:
Admin status  : Disabled,
File          : saa.xml,
Interval      : 20
```

output definitions

Admin status	The status (Enabled or Disabled) of SAA XML history file generation.
File	The name of the XML file to which SAA writes session history entries.
Interval	The amount of time, in minutes, between each generation of the XML history file.

Release History

Release 7.3.2; command was introduced.

Related Commands

saa xml	Configures SAA XML file generation parameters.

MIB Objects

```
alaSaaXmlFeature
   alaSaaXmlStatus
   alaSaaXmlFilename
   alaSaaXmlInterval
```

show saa statistics

Display SAA statistics.

show saa [*string***] statistics [aggregate | history]**

Syntax Definitions

string	An existing SAA ID string.
aggregate	Displays aggregate results for the specified SAA.
history	Displays a results history for the specified SAA.

Defaults

By default, statistics are displayed for all SAAs and only for the most recent SAA test run.

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- If the **aggregate** parameter is specified, then only the aggregate results are displayed.
- If the **history** parameter is specified, then only the history results are displayed.
- Since results are only kept for the last five iterations, using the **history** option displays only the last five iterations of each SAA test and in each SAA history, iteration information of first 20 received packets are stored.
- Specify the SAA ID to display statistics for a specific SAA.
- Statistics and history do not persist across a switch reboot or takeover.

Examples

```
-> show saa statistics
Legend: eth-lb  = ethoam-loopback
        eth-dmm = ethoam-two-way-delay
        - = Delay or jitter value not available

Aggregate Record:
SAA  Owner  Type   Time of Last-Run    RTT  RTT  RTT  RTT Jitter Jitter Jitter Jitter Packets
Description
                                        Min  Avg  Max  Thr  Min  Avg  Max  Thr  Sent Rcvd
----+-----+-----+--------------------+----+----+----+----+----+----+----+----+---+---+-----
saa1 USER ip-ping 2013-06-19,12:52:52.0 970 1067 1432  -    1    99  455   -    7   7 DEFAULT
saa2 USER ip-ping 2013-06-19,11:06:02.0 192  238  383  200  15   62  191  150   5   5 DEFAULT
saa3 USER eth-dmm 2013-06-19,12:52:25.0 1563 2654 3574  -   15   27  173    -   5   5 DEFAULT
saa4 USER eth-lb  2013-06-19,22:30:40.0 1243 1537 2166 100  23   42   96  500   6   6 DEFAULT
```

```
-> show saa statistics history
Legend: eth-lb  = ethoam-loopback
        eth-dmm = ethoam-two-way-delay
        - = Delay or jitter value not available

History Records SAA: saa1
Type    Time of Last-Run      RTT  RTT  RTT  RTT Jitter Jitter Jitter Jitter Packets Result Descr
                              Min  Avg  Max  Thr  Min  Avg  Max  Thr Sent Rcvd
-------+--------------------+----+----+----+----+----+----+----+----+---+---+-------+-------
ip-ping 2013-06-19,14:06:08.0 175  205  281  500    4   39  106  150   5   5  success DEFAULT
ip-ping 2013-06-19,14:04:26.0 171  209  307  500   11   51  125  150   5   5  success DEFAULT
ip-ping 2013-06-19,13:36:02.0 181  199  245  500    1   23   64  150   5   5  success DEFAULT
ip-ping 2013-06-19,11:06:02.0 192  238  383  500   15   62  191  150   5   5  success DEFAULT

-> show saa ip-ping statistics aggregate
SAA: ip-ping

  Total numbers of iterations : 4
    Aggregated Record:
      Total Packets Sent                 : 20,
      Total Packets Received             : 20,
      Avg RTT-Min/Avg/Max (micro sec)    : 171/212/383,
      Avg Jitter-Min/Avg/Max (micro sec) : 1/43/191,
      Timestamp-Min RTT                  : 2013-06-19,14:04:26.0,
      Timestamp-Max RTT                  : 2013-06-19,11:06:02.0,
      Timestamp-Min Jitter               : 2013-06-19,13:36:02.0,
      Timestamp-Max Jitter               : 2013-06-19,11:06:02.0
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.2: **Owner**, **RTT Thr**, and **Jitter Thr** fields added.

Related Commands

saa	Configures a SAA.

MIB Objects

```
alaSaaIpResultsTable
   alaSaaIpResultsPktsSent
   alaSaaIpResultsPktsRcvd
   alaSaaIpResultsRunResultReason
   alaSaaIpResultsRunTime
   alaSaaIpResultsMinRTT
   alaSaaIpResultsAvgRTT
   alaSaaIpResultsMaxRTT
   alaSaaIpResultsMinJitter
   alaSaaIpResultsAvgJitter
   alaSaaIpResultsMaxJitter
alaSaaEthoamResultsTable
   alaSaaEthoamResultsPktsSent
   alaSaaEthoamResultsPktsRcvd
   alaSaaEthoamResultsRunResultReason
   alaSaaEthoamResultsRunTime
   alaSaaEthoamResultsMinRTT
   alaSaaEthoamResultsAvgRTT
   alaSaaEthoamResultsMaxRTT
   alaSaaEthoamResultsMinJitter
   alaSaaEthoamResultsAvgJitter
   alaSaaEthoamResultsMaxJitter
alaSaaIpCtrlTable
   alaSaaIpCtrlTotalPktsSent
   alaSaaIpCtrlTotalPktsRcvd
   alaSaaIpCtrlMinRTT
   alaSaaIpCtrlAvgRTT
   alaSaaIpCtrlMaxRTT
   alaSaaIpCtrlMinJitter
   alaSaaIpCtrlAvgJitter
   alaSaaIpCtrlMaxJitter
alaSaaEthoamCtrlTable
   alaSaaEthoamCtrlTotalPktsRcvd
   alaSaaEthoamCtrlTotalPktsSent
   alaSaaEthoamCtrlMinRTT
   alaSaaEthoamCtrlAvgRTT
   alaSaaEthoamCtrlMaxRTT
   alaSaaEthoamCtrlMinJitter
   alaSaaEthoamCtrlAvgJitter
   alaSaaEthoamCtrlMaxJitter
```

57 CMM Commands

The Chassis Management Module (CMM) CLI commands permit you to manage switch software files on the CMM.

MIB information for the CMM commands is as follows:

Filename: ALCATEL-IND1-CHASSIS-MIB.mib
Module: alcatelIND1ChassisMIB

Filename: ALCATEL-IND1-CONFIG-MGR-MIB DEFINITIONS.mib
Module: alcatelIND1ConfigMgrMIB

A summary of available commands is listed here:

reload secondary

Reloads the secondary CMM from the ***certified*** directory.

reload [chassis-id *chassis***] secondary [in [***hours***:] ***minutes* **| at** *hour***:***minute* **[***month day* | *day month***]]**

reload secondary cancel

Syntax Definitions

chassis	The chassis identifier.
in [*hours***:]** *minutes*	Optional syntax. Schedules a reload of the software to take effect in the time. The time can be specified in minutes or hours and minutes within the next 24 hours.
at *hour***:***minute*	Optional syntax. Schedules a reload of the software to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes place on the following day.
month day | *day month*	The name of the month and the number of the day for the scheduled reload. Specify a month name and the day number. See examples below for further explanation.
cancel	Cancels a pending time delayed reboot.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Can be issued from both primary or secondary CMM.
- Reloads the secondary CMM only, the Primary CMM remains operational.

Examples

```
-> reload secondary
-> reload secondary in 15:25
-> reload secondary at 15:25 august 10
-> reload secondary at 15:25 10 august
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload from	Reloads both CMMs from the specified directory.

MIB Objects

```
chasEntPhysicalTable
   csEntPhysicalIndex
   chasEntPhysAdminStatus
chasControlRedundantTable
   chasControlDelayedRebootTimer
```

reload all

Reloads both Chassis Management Modules (CMMs) from the ***certified*** directory.

reload [chassis-id *chassis***] all [in [***hours***:]** *minutes* **|** **at** *hour***:***minute* **[***month day* | *day month***]]**

reload all cancel

Syntax Definitions

chassis	The chassis identifier.
in [*hours***:]** *minutes*	Optional syntax. Schedules a reload of all modules to take effect in the specified minutes or hours and minutes within the next 24 hours.
at *hour***:***minute*	Optional syntax. Schedules a reload of all modules to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes place on the following day.
month day | *day month*	The name of the month and the number of the day for the scheduled reload. Specify a month name and the day number. It is unimportant if the month or day is first. See examples below for further explanation.
cancel	Cancels a pending time delayed reload.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Can be issued from the Primary CMM only.

Examples

```
-> reload all
-> reload all in 1:30
-> reload all at 12:00 july 25
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload slot	Reloads a specific NI module.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
chasGlobalControl
   chasGlobalControlDelayedResetAll
```

reload from

Reloads both CMMs from the specified directory. There is no CMM failover during this reboot, causing a loss of switch functionality during the reboot. All the NIs and the secondary CMM will reload.

reload [chassis-id *chassis***] from** *image_dir* **{rollback-timeout** *minutes* **| no rollback-timeout [in [***hours:***]** *minutes* **| at** *hour:minute***] [redundancy-time** *minutes***]}**

Syntax Definitions

chassis	The chassis identifier when running in virtual chassis mode.
image_dir	The directory that contains the image files to be loaded onto the switch.
rollback-timeout *minutes*	Sets a timeout period, in minutes. The switch immediately reboots from the specified directory. At the end of this time period, the switch automatically reboots again from the ***certified*** directory. The valid range of rollback timeout minutes is 1–15.
no rollback-timeout	Specifies no timeout to rollback. If the command is issued with this keyword, then the switch continues to run from the specified directory until manually rebooted.
in [*hours***:]** *minutes*	Optional syntax. Schedules a reload of the to take effect in the specified minutes or hours and minutes within the next 24 hours.
at *hour***:***minute*	Optional syntax. Schedules a reload to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes place on the following day.
redundancy-time *minutes*	Specifies the time period in minutes that the switch must run without failure. If a failure occurs within this time period, the switch will reboot from the ***certified*** directory.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Can be issued from Primary CMM only.
- This command is used to reload the switch from the specified directory.
- A file verification will be performed before rebooting to ensure all necessary files are present and valid. An error message will be displayed describing any issues found.
- The image directory reload takes place immediately unless a time frame is set using the **in** or **at** keywords.

- If a rollback-timeout is set, the switch reboots again after the set number of minutes, from the **certified** directory. The reboot can be halted by issuing a cancel order as described in the **reload all** command.
- If the **redundnacy-time** parameter is entered, any reboot of the Primary CMM prior to the redundnacy timer expiring will cause the switch to reboot. If the Primary CMM reboots after the redundancy timer expires, the secondary CMM will take over without a reboot.

Examples

```
-> reload working rollback-timeout 5
-> reload working no rollback-timeout
-> reload working no rollback-timeout in 50
-> reload working rollback-timeout 10 at 12:50
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload all	Reboots both CMMs from the ***certified*** directory.

MIB Objects

```
chasControlModuleTable
   chasControl
   chasControlVersionMngt
   chasControlActivateTimeout
   chasControlRedundancyTime
   chasControlDelayedActivateTimer
   chasControlWorkingVersion
   chasControlNextRunningVersion
```

reload slot

Reloads the NI in the specified slot using the current running image.

reload slot *chassis/slot*

Syntax Definitions

chassis	The chassis identifier.
slot	The slot number to be reloaded.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

Can be issued from Primary CMM only.

Examples

```
-> reload slot 1/2
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload from	Reloads both CMMs from the specified directory.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
```

reload chassis-id

Reloads the specified chassis id when running in virtual chassis mode.

reload chassis-id *chassis* **[all] [in [***hours***:]** *minutes* **| at** *hour***:***minute* **[***month day* | *day month***]]**

reload chassis-id cancel

Syntax Definitions

chassis	The chassis identifier.
in [*hours***:]** *minutes*	Optional syntax. Schedules a reload of the software to take effect in the time. The time can be specified in minutes or hours and minutes within the next 24 hours.
at *hour***:***minute*	Optional syntax. Schedules a reload of the software to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes place on the following day.
month day | *day month*	The name of the month and the number of the day for the scheduled reload. Specify a month name and the day number. See examples below for further explanation.
cancel	Cancels a pending time delayed reboot.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Can be issued from both primary or secondary CMM.
- Reloads the secondary CMM only, the Primary CMM remains operational.

Examples

```
-> reload chassis-id 1
-> reload chassis-id 1 in 15:25
-> reload chassis-id 1 at 15:25 august 10
-> reload chassis-id 1 at 15:25 10 august
-> reload chassis-id 1 cancel
```

Release History

Release 7.3.1; command introduced.

Related Commands

reload from	Reloads both CMMs from the specified directory.

MIB Objects

```
chasEntPhysicalTable
   csEntPhysicalIndex
   chasEntPhysAdminStatus
chasControlRedundantTable
   chasControlDelayedRebootTimer
```

copy certified

Copies the contents of the ***certified*** directory to the specified directory.

copy certified *image_dir* **[make-running-directory]**

Syntax Definitions

image_dir	The directory that the contents of the ***certified*** directory will be copied to.
make-running-directory	Makes the destination directory the new RUNNING DIRECTORY after the configuration is copied.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Using the **make-running-directory** parameter changes the RUNNING DIRECTORY allowing changes to be saved using the **write memory** command.
- This command does not delete any extra files in the target directory.
- This command does not affect the synchronization status of the running configuration.
- To synchronize the running and saved configuration, use the **write memory** command.

Examples

```
-> copy certified mydir
-> copy certified mydir make-running-directory
```

Release History

Release 7.1.1; command introduced.

Related Commands

copy flash-synchro	Copies the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
chasControlModuleTable
   chasControlVersionMngt
   chasControlWorkingVersion
```

issu from

Upgrades the system with the images stored in the specified directory with minimal disruption to traffic.

issu from *image_dir* **[redundancy-time** *minutes***]**

Syntax Definitions

image_dir	Specifies the pathname for the directory that contains the image files.
redundancy-time *minutes*	This parameter is not supported with the **issu** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The new code must support ISSU with the current running version of code.
- A text file named '*issu_version*' is used to determine ISSU compatibility between code versions. It can be downloaded from the Service and Support website and must be included in the directory along with the new image files.

Examples

```
-> issu from myissu
```

Release History

Release 7.1.1; command introduced.

Related Commands

issu slot	Causes a power-cycle of the NI in the specified slot after an ISSU upgrade.

MIB Objects

```
chasEntModuleTable
   chasControlWorkingVersion
   chasControlRedundancyTime
```

issu slot

Causes a reset of the NI in the specified slot after an ISSU upgrade.

issu slot *num*

Syntax Definitions

num	Specifies the slot number.

Defaults

N/A

Platforms Supported

OmniSwitch 9900

Usage Guidelines

Will return an error if ISSU is not in progress or if the slot has already been reset after the ISSU.

Examples

```
-> issu slot 2
```

Release History

Release 7.1.1; command introduced.

Related Commands

issu from	Upgrades the system with the images stored in the specified directory without disruption to traffic.

MIB Objects

```
chasEntPhysicalTable
   entPhysicalIndex
```

write memory

Copies the current configuration (RAM) to the RUNNING DIRECTORY on the primary CMM.

write memory [flash-synchro]

Syntax Definitions

flash-synchro	Synchronizes the primary and secondary CMM.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to copy the changes performed using the CLI commands from the running configuration (RAM) to the RUNNING DIRECTORY.
- The **flash-synchro** keyword synchronizes the files between the primary and secondary CMMs by overwriting the contents of the secondary CMM ***certified*** directory with the contents of the primary CMM certified directory.
- This command is only valid if the switch isn't running from the ***certified*** directory. Use the **show running-directory** command to check where the switch is running from.
- During flash synchronization configuration changes may time out causing error messages to be displayed. Once the synchronization is complete configuration changes can resume.

Examples

```
-> write memory
-> write memory flash-synchro
```

Release History

Release 7.1.1; command introduced.

Related Commands

copy flash-synchro	Copies the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
configManager
   configWriteMemory
```

copy running certified

Copies the current RUNNING DIRECTORY configuration to the ***certified*** directory on both CMMs.

copy running certified [flash-synchro]

Syntax Definitions

flash-synchro	Synchronizes the primary and secondary CMM.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command is used to overwrite the contents of the ***certified*** directory with the configuration from the RUNNING DIRECTORY. This should only be done if the running configuration has been verified.
- This command only synchronizes the image and configuration files in the RUNNING DIRECTORY, no other directories, such as the **switch** or **network** directories, are synchronized.
- The **flash-synchro** keyword synchronizes the files between the primary and secondary CMMs by overwriting the contents of the secondary CMM ***certified*** directory with the contents of the primary CMM ***certified*** directory. Beginning in 7.3.1 the flash-synchro functionality is done automatically; entering the **flash-synchro** parameter is no longer required.
- In 7.3.3 the flash-synchro parameter will display an error on the OS6900 is there is no secondary CMM.
- If there is not enough free space, the copy attempt fails and an error message is generated.
- This command does not work if the switch is running from the ***certified*** directory. To view where the switch is running from, see the **show running-directory** command.
- This command may take up to two minutes to complete.

Examples

```
-> copy running certified
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; **flash-synchro** parameter no affect; the functionality is performed automatically.

Related Commands

copy flash-synchro	Copies the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
chasControlModuleTable
   chasControlVersionMngt
   chasControlWorkingVersion
```

modify running-directory

Changes the RUNNING DIRECTORY to the specified directory.

modify running-directory *image_dir*

Syntax Definitions

image_dir	The directory name to become the new RUNNING DIRECTORY.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to change the RUNNING DIRECTORY and allow configuration changes to be saved to the new RUNNING DIRECTORY.

Examples

```
-> modify running-directory user-config1
-> write memory
```

Release History

Release 7.1.1; command introduced.

Related Commands

write memory	Copies the running primary RAM version of the CMM software to the RUNNING DIRECTORY.

MIB Objects

```
chasControlModuleTable
   CurrentRunningVersion
```

copy flash-synchro

Copies the ***certified*** directory version of the primary CMM software to the ***certified*** directory of the secondary CMM.

copy flash-synchro

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is used to synchronize the ***certified*** directories of the primary and secondary CMMs. The two CMMs must be synchronized if a fail over occurs, otherwise switch performance is affected.
- This command is a shorter version of the '**copy running certified flash-synchro**' command. Beginning in 7.3.1 the flash-synchro functionality is done automatically; this command is no longer required.

Examples

```
-> copy flash-synchro
-> configure copy flash-synchro
```

Release History

Release 7.1.1; command introduced.

Related Commands

copy running certified	Copies the RUNNING DIRECTORY configuration to the ***certified*** directory on the primary CMM.

MIB Objects

```
chasControlModuleTable
   chasControlVersionMngt
```

takeover

Forces the current secondary CMM to assume the role of the primary CMM.

takeover [*chassis***]**

Syntax Definitions

chassis	The chassis identifier.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command causes the secondary CMM to take over the functions of the primary CMM. After this command, the old primary CMM is the new secondary CMM.
- Be sure that the secondary CMM has all software (i.e., image and configuration files) required to continue CMM operations, before issuing the **takeover** command.
- For information on synchronizing the primary and secondary CMM software before issuing the **takeover** command, see the **copy flash-synchro** command.

Examples

```
-> takeover
```

Release History

Release 7.1.1; command introduced.

Related Command

reload all	Reboots the switch.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
```

show running-directory

Shows the current state of version and configuration management for a CMM.

show running-directory

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Once a switch boots up and is running, it runs either from the ***working, certified***, or a *user-defined* directory. If the switch is running from the ***certified*** directory, changes made to the RUNNING CONFIGURATION using CLI commands, cannot be saved.
- Depending on the switch configuration there may be a small delay before the information is displayed.

Examples

```
-> show running-directory

CONFIGURATION STATUS
  Running CMM              : PRIMARY,
  CMM Mode                 : MONO CMM,
  Current CMM Slot         : A,
  Running configuration    : CERTIFIED,
  Certify/Restore Status   : CERTIFIED,
SYNCHRONIZATION STATUS
  Flash Between CMMs       : SYNCHRONIZED
  Running Configuration    : SYNCHRONIZED
BOOT STATUS
  Machine State            : SHUTDOWN
```

output definitions

Running CMM	The CMM currently controlling the switch, either PRIMARY or SECONDARY.
CMM Mode	Whether there are one or two CMMs installed or Virtual Chassis mode.
Current CMM Slot	The slot of the primary CMM, A or B.
Running Configuration	The current RUNNING DIRECTORY.
Certify/Restore Status	Indicates if the CMM has been certified.

output definitions (continued)

Flash Between CMMs	**SYNCHRONIZED**: Flash between CMMs is identical. **NOT SYNCHRONIZED**: Flash between CMMs is not identical.
Running Configuration	**SYNCHRONIZED**: RUNNING CONFIGURATION has been saved to the RUNNING DIRECTORY. **NOT SYNCHRONIZED**: RUNNING CONFIGURATION has not been saved to the RUNNING DIRECTORY.
Machine State	**SHUTDOWN -** When in VC mode, this indicates the chassis has shutdown due to the 'virtual-chassis shutdown' command or when the chassis has shutdown due to a VC error. It is only displayed if the chassis is in the shutdown state.

Release History

Release 7.1.1; command introduced.

Related Commands

reload all	Reboots the switch.
copy flash-synchro	Copies the ***certified*** directory version of the primary CMM software to the ***certified*** directory of the secondary CMM.

MIB Objects

```
chasControlModuleTable
   chasControlSynchronizationStatus
   chasControlCertifyStatus
   chasControlRunningVersion
chasEntPhysicalTable
   chasEntPhysOperStatus
   entPhysicalIndex
chasControlReloadTable
   chasControlReloadStatus
```

show reload

Shows the status of any time delayed reboot(s) that are pending on the switch.

show reload [[chassis-id *chassis***] [status | all status]**

Syntax Definitions

chassis	The chassis identifier.
status	Displays whether or not either of the CMMs are scheduled for a reload.
all status	Displays whether or all the modules are scheduled for a reload.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- It is possible to preset a reboot on a CMM by using the **reload** command. If this is done, use the **show reload** command to see when the next scheduled reboot is going to occur.
- If the **reload from** command is used, and a rollback timeout is set, the rollback occurs and is shown using the **show reload** command.

Examples

```
-> show reload status
Primary   Control Module Reload Status: No Reboot Scheduled,
Secondary Control Module Reload Status: No Reboot Scheduled
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload secondary	Reboots the primary or secondary CMM to its startup software configuration.
reload from	Immediate primary CMM reboot to the specified software configuration without secondary CMM takeover.

MIB Objects

```
chasControlModuleTable
   chasControlDelayedActivateTimer
chasGlobalControl
   chasGlobalControlDelayedResetAll
```

show microcode

Displays microcode versions installed on the switch.

show microcode [working | certified | loaded | issu | *image_dir***]**

Syntax Definitions

working	Specifies the ***working*** directory.
certified	The chassis identifier when running in virtual chassis mode.
loaded	Specifies the loaded (i.e., currently-active) microcode versions.
issu	Specifies the ***issu*** directory.
image_dir	Specifies the *user-defined* directory.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If no additional parameters are entered microcode information for the RUNNING CONFIGURATION is displayed.

Examples

```
-> show microcode
Package           Release       Size     Description
------------------+---------------+--------+----------------------------------
Ros.img           7.1.1.403.R01    1828255 Alcatel-Lucent OS
Reni.img          7.1.1.403.R01    1359435 Alcatel-Lucent NI
```

output definitions

Package	File name.
Release	Version number.
Size	File size.
Description	File description.

Release History

Release 7.1.1; command introduced.

Related Commands

usb	Displays the archive history for microcode versions installed on the switch.

MIB Objects

N/A

usb

Enables access to the device connected to the USB port.

usb {enable | disable}

Syntax Definitions

N/A

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Must use an Alcatel-Lucent Enterprise certified USB device.
- If an Alcatel-Lucent Enterprise certified USB device is connected after enabling the USB interface, the device will be automatically mounted as **/uflash**.
- Once mounted, common file and directory commands can be used for file management.

Examples

```
-> usb enable
-> cp /flash/working/boot.cfg /uflash/boot.cfg
-> ls /uflash
```

Release History

Release 7.1.1; command was introduced.

Related Commands

MIB Objects

usb auto-copy	Allows backup image files from the USB device to be automatically copied to the /flash/working directory on the switch immediately after the USB device is connected
usb backup admin-state	Enables or disables USB backup on the switch.

MIB Objects

```
systemServices
   systemServicesUsbEnable
```

usb backup admin-state

Enables or disables USB backup on the switch.

usb backup admin-state {enable | disable} [key *string* **| hash-key** *string***]**

Syntax Definitions

enable	Enables Administrative control to USB backup on the switch
disable	Disables Administrative control to USB backup on the switch
key	Keyword which will be used for encryption. *This parameter is only supported on the OmniSwitch 6465.*
hash-key	Keyword which will be decrypted and then used for encryption. *This parameter is only supported on the OmniSwitch 6465.*

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- When this command is enabled, the images and configuration from certified and running directories are copied into */uflash/6860/certified* and */uflash/6860/running* directories.
- When **write memory** is executed and backup is enabled, the configuration files and images from */flash/running-directory* are copied to */uflash/6860/running-directory name*
- When **usb backup admin-state** is enabled and **copy running certified** and **write memory flash-synchro** commands are executed, the configuration and images from */flash/certified* will be copied to */uflash/6860/certified.*
- Encryption is supported only on the OmniSwitch 6465.
  - When a key or hash key is specified, all of the configuration files and images will be encrypted and copied to the USB device.
  - If a key or hash key is not specified, all of the configuration files and images will be copied as is to the USB device.
  - Maximum length of key should be 32 characters. Minimum key length should be 8 characters.
  - If the user has gone through one back up cycle of encryption and wants to disable encryption, then the user must disable the USB back up and enable it again with no password.
- On the OmniSwitch 6465, when power supply configurations are added by the **powersupply enable** command, the power supply configurations are backed up in */uflash/6465/system* folder when backup is enabled.

- Back-up cannot be enabled if auto-copy is enabled and auto-copy cannot be enabled if back-up is enabled. So only one of these features can be enabled at any given time.

Examples

```
-> usb backup admin-state enable
-> usb backup admin-state disable
-> usb backup admin-state enable key “abc12345”
-> usb backup admin-state enable hash-key “a05234d”
```

Release History

Release 8.5R1; command was introduced.
Release 8.5R2; **key** and **hash-key** parameter added.

Related Commands

usb auto-copy	Allows backup image files from the USB device to be automatically copied to the /flash/working directory on the switch immediately after the USB device is connected
usb	Enables access to the device connected to the USB interface.

MIB Objects

```
systemServices
   systemServicesUsbBackupAdminState
   systemServicesUsbBackupKey
   systemServicesUsbBackupHashkey
```

usb auto-copy

Allows the image files from the USB device to be automatically copied to the switch immediately after the USB device is connected.

usb auto-copy {enable | disable} copy-config {enable| disable} [key *string* **| hash-key** *string* **]**

Syntax Definitions

enable	Enables Administrative control to USB auto copy on the switch
disable	Disables Administrative control to USB auto copy on the switch
key	Keyword which will be used for encryption. *This parameter is only supported on the OmniSwitch 6465.*
hash-key	Keyword which will be decrypted and then used for encruption. *This parameter is only supported on the OmniSwitch 6465.*

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

- If the automatic copy is successful the switch will automatically reboot.
- The USB device must contain the proper file structure and image files mentioned below and the USB root directory must contain a signature file named *aossignature*. The *aossignature* file can be a blank text file transferred to the switch.
- This operation will enable all of the image files from the */uflash/6465/working* or */uflash/6860/working* directory to be copied to the */flash/working* directory.
- If the auto-copy is successful, the auto-copy feature will be disabled before rebooting the switch and must be re-enabled by the administrator for the next auto-copy process to execute. This will prevent running the same auto-copy multiple times.
- If **copy-config** is enabled, configuration files will also be copied in addition to image files to the */flash/working* directory from */uflash/6860/working* directory.
- Encryption is supported only on the OmniSwitch 6465.
  - When a key or hash key is specified, all of the configuration files and images will be decrypted and copied to the AOS flash.
  - If a key or hash key is not specified, all of the configuration files and images will be copied as is to the AOS flash.
  - Maximum length of key should be 32 characters. Minimum key length should be 8 characters.

- On the OmniSwitch 6465, when power supply configurations are added by the **powersupply enable** command, the power supply configurations are backed up in */uflash/6465/system* folder when backup is enabled.
- Back-up cannot be enabled if auto-copy is enabled and auto-copy cannot be enabled if back-up is enabled. So only one of these features can be enabled at any given time.

Examples

```
-> usb auto-copy enable copy-config enable
-> usb auto-copy enable copy-config disable
-> usb auto-copy enable copy-config enable key “abc12345”
-> usb auto-copy enable copy-config enable hash-key “a05234d”
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R1; **copy-config** parameter added.
Release 8.5R2; **key** and **hash-key** parameter added.

Related Commands

usb	Enables access to the device connected to the USB interface.
usb backup admin-state	Enables or disables USB backup on the switch.

MIB Objects

```
systemServices
   systemServicesUsbCopyConfig
   systemServicesUsbBackupKey
   systemServicesUsbBackupHashkey
```

mount

Mounts a USB device on /uflash.

mount [/uflash]

Syntax Definitions

/uflash	The name of the file-system to mount.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

Once the USB device is mounted most file and directory commands associated with the **/flash** file system can be used with **/uflash** such as: mkdir, rmdir, cd, rm, cp, ls.

Examples

```
-> mount /uflash
-> ls /uflash
```

Release History

Release 7.1.1; command was introduced.

Related Commands

umount	Unmounts the /uflash file system from AOS.

MIB Objects

```
systemServicesAction
   systemServicesArg1
```

umount

Unmounts the /uflash file system from AOS.

umount /uflash

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

This command unmounts the USB drive and should be used prior to unplugging the USB drive to prevent possible data corruption.

Examples

```
-> umount /uflash
```

Release History

Release 7.1.1; command was introduced.

Related Commands

mount	Mounts the /uflash file system from AOS.

MIB Objects

```
systemServicesAction
   systemServicesArg1
```

show usb statistics

Displays the status USB setting and features.

show usb statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 9900

Usage Guidelines

N/A

Examples

```
-> show usb statistics
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sdb1               500732    261216    239516  52% /vroot/uflash
   Host scsi6: usb-storage
       Vendor: Alcatel-Lucent
      Product: USB
Serial Number: AA04012700031693
     Protocol: Transparent SCSI
   Transport: Bulk
         usb: enabled
usb auto-copy: disable
auto-copy in progress: No
```

output definitions

usb	Status of USB device interface.
usb auto-copy	Status of USB auto-copy feature.
auto-copy in progress	Is the switch currently in the process of performing an auto-upgrade.

Release History

Release 7.1.1; command was introduced.

Related Commands

usb	Enables access to the device connected to the USB interface.
usb auto-copy	Allows backup files from the USB device to be automatically copied to the switch switch immediately after the USB device is connected.
mount	Mounts the /uflash file system.

MIB Objects

```
systemServices
   systemServicesUsbEnable
   systemServicesUsbAutoCopyEnable
   systemServicesUsbDisasterRecoveryEnable
```

show issu status

Displays the status of ISSU.

show issu status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show issu status
Slot     ISSU-Status
-------+-----------------+
 1       ISSU Pending
 2       ISSU Pending
 3       ISSU Pending

-> show issu status
Slot     ISSU-Status
-------+-----------------+
 1       ISSU Complete
 2       ISSU Complete
 3       ISSU Complete
```

output definitions

Slot	Specifies the slot number.
ISSU-Status	Indicates the ISSU status for a slot: **Pending** - Slot has not been reset; upgrade is not complete. **Complete** - Slot has been reset; upgrade is complete.

Release History

Release 7.1.1; command was introduced.

Related Commands

issu from	Upgrades the system with the images stored in the specified directory without disruption to traffic.

MIB Objects

N/A

auto-config-abort

Aborts the Automatic Remote Configuration download process.

auto-config-abort

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to stop the Automatic Remote Configuration download process.

Examples

```
-> auto-config-abort
```

Release History

Release 7.3.4; command was introduced.

Related Commands

N/A

MIB Objects

N/A

image integrity check

Verifies whether the SHA256 hash key of an image file located in the specified directory matches the SHA256 hash key in the specified key file.

image integrity check *image_dir* **key-file** *filename*

Syntax Definitions

image_dir	The directory on the switch that contains the image file to verify. Enter the name of the directory in "/flash" or include the full path (for example, "working" or "/flash/working").
filename	The name of the file that contains the key for the image file in the specified directory. Enter the name of the key file or include the full path (for example, "hash.txt" or "/flash/hash.txt").

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the name of the key file is specified without the directory path, the switch will look for the key file in the same directory specified for the image file.
- The following format is used to store the hash key values in the key file:
  Uos.img:f0ff173eff38e43e0598663da2185a363fcba5bd407201d7537d0a6b9f58670e

Example

```
-> image integrity check /flash/working key-file /flash/hash.txt
This operation may take several minutes...

Success: Key matched.
```

Release History

Release 8.3.1; command introduced.

Related Commands

image integrity get-key	Calculates and displays the SHA256 key for image files.

MIB Objects

```
systemServicesAction
systemServicesArg1
systemServicesArg2
```

image integrity get-key

Displays the SHA256 hash key of the image present in the specified location.

image integrity get-key *image_dir*

Syntax Definitions

image_dir	The directory on the switch that contains the image file. Enter the name of the directory in "/flash" or include the full path (for example, "working" or "/flash/working").

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When this command is entered, the SHA256 hash of the image files in the specified directory is calculated and displayed. It can be manually verified against the hash provided in the file.
- To store the hash key value in a text file that can be used with the **image file integrity check** command, use the following format:
  Uos.img:f0ff173eff38e43e0598663da2185a363fcba5bd407201d7537d0a6b9f58670e

Example

```
-> image integrity get-key /working
This operation may take several minutes...

Image Name                  SHA256 Key
----------------+-----------------------------------------
Uos.img           c64d6b23312a6f9c4b99642b31ed0e87e600bce58d6fdd089d09e1f8077bd208

-> image integrity get-key /flash/certified
This operation may take several minutes...

Image Name                  SHA256 Key
----------------+-----------------------------------------
Uos.img           3d4d488a73eb798325bacb5793ef0d67bdf377527278a6732270d3a4801bb44b
```

Release History

Release 8.3.1; command introduced.

Related Commands

image integrity check	Verifies the SHA256 hash key for the image file matches the key specified in a text file.

MIB Objects

```
systemServicesAction
systemServicesArg1
systemServicesArg2
```

58 Chassis Management and Monitoring Commands

Chassis Management and Monitoring commands allow you to configure and view hardware-related operations on the switch. Topics include basic system information, as well as Network Interface (NI) module and chassis management.

Additional Information. Refer to your separate *Hardware Users Guide* for detailed information on chassis components, as well as managing and monitoring hardware-related functions.

MIB information for the Chassis Management and Monitoring commands is as follows:

Filename: ALCATEL-IND1-CHASSIS-MIB.mib
Module: alcatelIND1ChassisMIB

Filename: ALCATEL-IND1-SYSTEM-MIB.mib
Module: alcatelIND1SystemMIB

Filename: ALCATEL-IND1-CAPMAN-MIB.mib
Module: alcatelIND1CapManMIB

A summary of available commands is listed here:

Management Commands	**system contact** **system name** **system location** **system date** **system time** **system timezone** **system daylight-savings-time** **update uboot** **update fpga-cpld** **reload slot** **power slot** **powersupply enable** **powersupply powersave** **powersupply type** **hash-control** **bluetooth** **capability profile** **capability profile tcam mode** **capability trap-threshold**
Monitoring Commands	**capability trap-threshold** **show system** **show hardware-info** **show chassis** **show cmm** **show slot** **show module** **show module long** **show module status** **show powersupply** **show fan** **show fantray** **show temperature** **show hash-control** **show bluetooth status** **show me** **show tcam utilization** **show tcam utilization detail** **show tcam app-groups** **show capability profile** **show pmd-files** **show tech-support** **show capability trap-threshold**
Licensing Commands	**license apply file** **show license-info**
Key Management Commands	**security key-chain gen-random-key** **security key** **security key-chain** **security key-chain key** **show security key** **show security key-chain**

Alarm Relay Commands	**alarm in** **alarm event** **alarm out** **alarm map** **alarm duration** **alarm clear status** **show alarm input config** **show alarm event config** **show alarm status**
Application Manager Commands	**appmgr** **appmgr list** **appmgr commit** **pkgmgr** **pkgmgr list** **pkgmgr commit**

system contact

Specifies the administrative contact for the switch. An administrative contact is the person or department in charge of the switch. If a contact is specified, users can easily find the appropriate network administrator if they have questions or comments about the switch.

system contact *text_string*

Syntax Definitions

text_string	The administrative contact being specified for the switch. The system contact can range from 1 to 254 characters in length. Text strings that include spaces must be enclosed in quotation marks. For example, **"Jean Smith Ext. 477 jsmith@company.com"**.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> system contact "Jean Smith Ext. 477 jsmith@company.com"
-> system contact engineering-test@company.com
```

Release History

Release 7.1.1; command introduced.

Related Commands

system name	Modifies the current system name of the switch.
system location	Specifies the current physical location of the switch.
capability trap-threshold	Displays the basic system information for the switch.

MIB Objects

```
system
   systemContact
```

system name

Modifies the current system name of the switch. The system name can be any simple, user-defined text description for the switch.

system name *text_string*

Syntax Definitions

text_string	The new system name. The system name can range from 1 to 32 characters in length. No spaces are allowed in the system name.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Spaces are not allowed in the system name.

Examples

```
-> system name OmniSwitch6900
-> system name OS6900
```

Release History

Release 7.1.1; command introduced.

Related Commands

system contact	Specifies the administrative contact of the switch (for example, an individual or a department).
system location	Specifies the current physical location of the switch.
capability trap-threshold	Displays the basic system information for the switch.

MIB Objects

```
system
   systemName
```

system location

Specifies the current physical location of the switch. If you need to determine the location of the switch from a remote site, entering a system location can be very useful.

system location *text_string*

Syntax Definitions

text_string	The physical location of the switch. For example, **TestLab**. The system location can range from 1 to 254 characters in length. Text strings that include spaces must be enclosed in quotation marks. For example, **"NMS Test Lab"**.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> system location "NMS Test Lab"
-> system location TestLab
```

Release History

Release 7.1.1; command introduced.

Related Commands

system contact	Specifies the administrative contact of the switch (for example, an individual or a department).
system name	Modifies the current system name of the switch.
capability trap-threshold	Displays the basic system information for the switch.

MIB Objects

```
system
   systemLocation
```

system date

Displays or modifies the current system date on the switch.

system date [*mm/dd/yyyy***]**

Syntax Definitions

mm/dd/yyyy	The new date being specified for the system. Enter the date in the following format: *mm/dd/yyyy*, where *mm* is the month, *dd* is the day, and *yyyy* is the year. For example, **08/08/2005**.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If you do not specify a new system date in the command line, the current system date is displayed.
- For more information on setting time zone parameters (for example, Daylight Savings Time), refer to the **system timezone** command on page 58-9.

Examples

```
-> system date 08/08/2010
-> system date
08/08/2010
```

Release History

Release 7.1.1; command introduced.

Related Commands

system time	Displays or modifies the current system time on the switch.
system timezone	Displays or modifies the time zone for the switch.

MIB Objects

```
systemServices
   systemServicesDate
```

system time

Displays or modifies the switch current system time.

system time [*hh:mm:ss***]**

Syntax Definitions

hh:mm:ss	The new time being specified for the system. To set this value, enter the current time in 24-hour format, where *hh* is the hour, *mm* is the minutes, and *ss* is the seconds. For example, **14:30:00**.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If you do not specify a new system time in the command line, the current system time is displayed.
- Setting the year to 1970 is not supported. The system interprets 1970 as meaning the internal clock has never been set and will reset to the year 2014.

Examples

```
-> system time 14:30:00
-> system time
14:30:08
```

Release History

Release 7.1.1; command introduced.

Related Commands

system date	Displays or modifies the current system date on the switch.
system timezone	Displays or modifies the time zone for the switch.

MIB Objects

```
systemServices
   systemServicesTime
```

system timezone

Displays or modifies the time zone for the switch.

system timezone [*timezone_abbrev***]**

Syntax Definitions

timezone_abbrev	Specifies a time zone for the switch and sets the system clock to run on UTC. If you specify a time zone abbreviation, the hours offset from UTC is automatically calculated by the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The configuration must be saved after changing the timezone.
- To display the current time zone for the switch, enter the syntax **system timezone**.
- If the configured timezone supports DST it is automatically enabled and cannot be disabled.
- If the configured timezone does not support DST it is automatically disabled and cannot be enabled.
- Refer to the *OmniSwitch AOS Release 8 Switch Management Guide* for a list of time zone abbreviations.

Examples

```
-> system timezone mst
```

Release History

Release 7.1.1; command introduced.

Related Commands

system date	Displays or modifies the current system date on the switch.
system time	Displays or modifies the current system time on the switch.

MIB Objects

```
systemServices
   systemServicesTimezone
   systemServicesTimezoneStartWeek
   systemServicesTimezoneStartDay
   systemServicesTimezoneStartMonth
   systemServicesTimezoneStartTime
   systemServicesTimezoneOffset
   systemServicesTimezoneEndWeek
   systemServicesTimezoneEndDay
   systemServicesTimezoneEndMonth
   systemServicesTimezoneEndTime
   systemServicesEnableDST
```

system daylight-savings-time

Displays the Daylight Savings Time (DST) setting for the configured timezone.

system daylight-savings-time [enable | disable]

Syntax Definitions

enable | disable enable

Defaults

parameter	default
Timezone supports DST	enabled
Timezone does not support DST	disabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the configured timezone supports DST it is automatically enabled.
- If the configured timezone does not support DST it is automatically disabled.

Examples

```
-> system daylight-savings-time
Daylight Savings Time (DST) is ENABLED.
```

Release History

Release 7.1.1; command introduced.

Related Commands

system time	Displays or modifies the current system time on the switch.
system timezone	Displays or modifies the timezone for the switch.
system date	Displays or modifies the current system date on the switch.

MIB Objects

```
systemServices
   systemServicesTimezone
   systemServicesEnableDST
```

update uboot

Updates the uboot versions of the CMM or NIs. Refer to the Release Notes and/or any available Upgrade Instructions for the new release before performing this type of update on the switch.

update uboot {cmm *slot* **| ni {all |** *slot***} file** *filename***}**

Syntax Definitions

cmm	Specifies that the update is performed for the Chassis Management Module (CMM)**.**
all	Specifies that the update is performed for all slots within a chassis.
slot	Specifies the slot number of the module within a chassis.
filename	Specifies the path and name of the upgrade file.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Note that when performing an update, it is important that the correct update file is used. Specifying the wrong file may impact the operation of the switch.

Examples

```
-> update uboot ni all file 9999.tar.gz
-> update uboot cmm 1 file /flash/temp/9999.tar.gz
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload slot	Reloads the specified NI module.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

update fpga-cpld

Updates the FPGA/CPLD versions of the CMM or NIs. Refer to the Release Notes and/or any available Upgrade Instructions for the new release before performing this type of update on the switch.

update fpga-cpld {cmm {*chassis/cmm* |*all*} **| ni {***chassis/ni* **| daughter** *num***} file** *filename***}**

Syntax Definitions

cmm	Specifies that the update is performed for the Chassis Management Module (CMM)**.**
daughter	Specifies the number of the daughter board on the NI module.
ni	Specifies the slot number of the module within a chassis.
filename	Specifies the path and name of the upgrade file.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Note that when performing an update, it is important that the correct update file is used. Specifying the wrong file may impact the operation of the switch.
- When updating CMMs with the **all** option an “fpga_kit” file must be used. If upgrading a CMM using the *chassis/cmm* option, a “vme” file must be used.

Examples

```
-> update fpga-cpld ni 4 file 9999.vme
-> update fpga-cpld cmm 1/1 file /flash/OS6865_U28X_CPLD_V11.vme
-> update fpga-cpld cmm all file fpga_kit_4960
```

Release History

Release 7.1.1; command introduced.
Release 7.3.4; **fpga** parameter changed to **fpga-cpld.**

Related Commands

reload slot	Reloads the specified NI module.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

reload slot

Reloads or reboots a specified Network Interface (NI) module.

reload slot *slot*

Syntax Definitions

slot	Specifies the slot number.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The **reload slot** command reboots only the specified NI. Other modules installed on the chassis, including primary and secondary CMMs, are not affected

Examples

```
-> reload slot 2
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload slot	Reloads the specified NI module.
power slot	Turns the power on or off for a specified Network Interface (NI) module.
show slot	Shows the hardware information and the current status for Network Interface (NI) modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   reset
```

power slot

Turns the power on or off for a specified Network Interface (NI) module.

power slot *chassis/slot*

no power slot *chassis/slot*

Syntax Definitions

chassis	The chassis identifier.
slot	The chassis slot number containing the NI module being powered on or off.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

Use the **no** form of this command to power off an NI module.

Examples

```
-> power slot 1
-> power slot 7
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload slot	Reloads the specified NI module.
show slot	Shows the hardware information and current status for Network Interface (NI) modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   powerOn
   powerOff
```

powersupply enable

Enables the power supply unit identified by the PSU-ID.

powersupply enable [*slot***]**

no powersupply enable [*slot***]**

Syntax Definitions

slot	Slot number of power supply.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

N/A

Release History

Release 7.1.1; command introduced.

Related Commands

power slot	Turns the power on or off for a specified Network Interface (NI) module.

MIB Objects

N/A

powersupply powersave

Enables the power saving functionality on the switch.

powersupply powersave {enable | disable}

Syntax Definitions

enable | disable	Enables or disables the power saving functionality.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

Not supported in this release.

Usage Guidelines

- When enabled unneeded power-supplies are shut down to conserve energy, only the power supplies required to provide N+1 redundancy remain on.
- If enabled and power is lost to all active power supplies simultaneously the switch will lose power since N+1 redundancy applies only to the active power supplies.
- If the power-save mode is disabled, all available power supplies are switched on at all times.

Examples

```
-> powersupply powersave disable
-> powersupply powersave enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show powersupply	Displays the hardware information and current status for chassis power supplies.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
```

powersupply type

Configures the type of power supply that is connected to the chassis.

powersupply *num* **name** *string* **type {ALE {lo-ac | hi-ac} | phoenix-contact {48VDC | 24VDC} | third-party wattage** *num***}** [**chassis-id** *chassis-id*]

Syntax Definitions

num	Power supply connector ID.
string	The descriptive name of the power supply.
lo-ac | hi-ac	The type of ALE power supply.
phoenix-contact 48VDC | 24VDC	The type of Phoenix Contact power supply.
third-party wattage *num*	The wattage value of the attached third-party power supply

Defaults

parameter	default
N/A	

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- The OmniSwitch 6465 cannot auto-detect the type of power supply connected. This command is used to configure the type of power supply that is connected.
- Refer to the OmniSwitch 6465 Hardware User Guide for chassis power requirements when using third-party power supplies.
- Refer to the OmniSwitch 6465 Hardware Users Guide for power supply specifications using the power supply part number mapping below. A power supply may be associated with multiple part numbers depending on ALE branding, ordering part number or manufacturer part number.
  - **lo-ac** (OS6465-BPN, PS-I75AC, SDR-75-48)
  - **hi-ac** (O6465-BPN-H, PS-I185AC-P, SDR-240-55)

Examples

```
-> powersupply 1 name ALE-75W-ps1 type ale lo-ac
-> powersupply 2 name ALE-75W-ps2 type ale lo-ac
-> powersupply 1 name third-party-ps type third-party wattage 75
```

Release History

Release 8.5 R1; command introduced.

Related Commands

show powersupply	Displays the hardware information and current status for chassis power supplies.

MIB Objects

N/A

hash-control

Configures the hash control method on the switch. Depending upon this configuration, hashing algorithm used by various applications for packet forwarding is affected.

hash-control {brief | extended [udp-tcp-port] | load-balance non-ucast {enable | disable}}

hash-control extended no udp-tcp-port

Syntax Definitions

brief	Sets hashing to brief mode.
extended	Sets hashing to extended mode.
udp-tcp-port	Sets extending hashing to use UDP/TCP ports.
enable | disable	Enables or disables the load balancing of non-unicast traffic on a link aggregate.

Defaults

parameter	default
hash-control	brief (OS6465, OS6900) extended (OS6560, OS6860, OS6865, OS9900)
udp-tcp-port	disabled
non-ucast	disabled

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Disabling TCP-UDP port hashing is recommended when Server Load Balancing (SLB) is configured, because SLB dynamically assigns ports.
- The hash control setting also impacts the fabric load balancing for Chassis based products. It is recommended not to set brief hashing mode on Chassis based products.
- Changing the hash control mode affects the hashing algorithm for Link Aggregation, Server Load Balancing and ECMP.
- The hashing mode must be set to extended to enable UDP/TCP port hashing.
- Enabling or disabling the **load-balance non-ucast** option applies to all link aggregates. When this option is disabled (the default), link aggregation load balances only unicast packets; all non-unicast packets are sent through the primary port of the link aggregate.
- When the **load-balance non-ucast** option is enabled, all non-unicast traffic (broadcast, L2 multicast, L3 multicast, and unknown unicast) is load balanced over the link aggregate.

Examples

```
-> hash-control brief
-> hash-control extended
-> hash-control extended udp-tcp-port
-> hash-control extended no udp-tcp-port
-> hash-control load-balance non-ucast enable
-> hash-control load-balance non-ucast disable
```

Release History

Release 7.2.1; command introduced.

Related Commands

show hash-control	Displays the current hash control setting for the switch.

MIB Objects

```
alaChasHashMode
alaChasUdpTcpPortMode
alachasNonUCHashControl
```

bluetooth

Enables or disables USB adapter with Bluetooth technology connectivity and configures the power level.

bluetooth {admin-state [enable | disable] | transmit-power [low | high]}

Syntax Definitions

enable | disable	Enables or disables USB adapter with Bluetooth technology connectivity.
low | high	Configures the power level to low or high.

Defaults

parameter	default
enable | disable	**enable**
low | high	**low**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

This command will configure all USB adapters with Bluetooth technology in a virtual chassis.

Examples

```
-> bluetooth admin-state enable
-> bluetooth transmit-power high
```

Release History

Release 8.1.1; command was introduced.

Related Commands

show bluetooth status	Displays the current USB adapter with Bluetooth technology settings.
show me	Executes an LED blink pattern for 10 seconds that is used by the USB adapter with Bluetooth technology to identify the connected switch.

MIB Objects

```
systemServices
   systemServicesUsbEnable
   systemServicesBluetoothTxPower
```

capability profile

Configures the mode of the switch to be either *switch* or *router*.

capability profile {switch | router}

Syntax Definitions

switch | router Configures the *switch* or *router* profile.

Defaults

parameter	default
switch | **router**	**switch**

Platforms Supported

OmniSwitch 6900-V72, 6900-C32, OmniSwitch 6900-X72

Usage Guidelines

- Use this command to change the mode of a switch between *switch* and a *router*. This will adjust the L2 and L3 table entries based on the network requirements.
- The *switch* profile provides more L2 entries. The *router* profile provides more LPM entries. Refer to the Specifications Guide for details on the L2 and L3 entries.
- The switch must be rebooted for the configured profile to take effect.

Examples

```
-> capability profile router
```

Release History

Release 8.5R2; command was introduced.

Related Commands

show capability profile Displays the active and configured profile settings.

MIB Objects

```
alaCapManProfile
   alaCapManProfileMode
```

capability profile tcam mode

Configures the TCAM (Ternary Content Addressable Memory) mode of the switch to support source IPv6 filtering.

capability profile tcam mode {source-ipv6 | dest-ipv6}

Syntax Definitions

source-ipv6	Selects the source IPv6 (enhanced) mode.
dest-ipv6	Selects the destination IPv6 mode.

Defaults

By default, the TCAM mode supports destination IPv6 filtering only; source IPv6 filtering is not allowed.

Platforms Supported

OmniSwitch 6560

Usage Guidelines

- Setting the TCAM mode to source IPv6 filtering is required to support DHCPv6 Snooping IPv6 source filtering on an OmniSwitch 6560.
- When the TCAM mode is changed, a warning message is displayed (see command examples below).
- After the TCAM mode is changed and the configuration is saved with the **write memory** command, reboot the switch to activate the specified mode.
- When the TCAM mode is set to source IPv6 filtering, the TCAM will operate in an enhanced mode to support the use of source IPv6 conditions in QoS policy rules.
- The following functionality is *not* supported when the source IPv6 filtering mode is active:
  - Destination IPv6 source filtering.
  - ISSU
  - QoS anti-spoofing
  - Fewer QoS policy rules supported.

Examples

```
-> capability profile tcam mode source-ipv6
WARNING: Source ipv6 tcam mode would not support : QoS policy with destination ipv6
address / destination network group / ipv6 Tcpflags.
Reboot is needed for the capability profile tcam mode to use source-ipv6

-> capability profile tcam mode dest-ipv6
WARNING: Destination ipv6 tcam mode would not support : QoS policy with source ipv6
address / source network group.
Reboot is needed for the capability profile tcam mode to use dest-ipv6
```

Release History

Release 8.6R1; command was introduced.

Related Commands

dhcpv6-snooping ipv6-source-filter	Configures the IPv6 source filtering capability for a port, link aggregate, or VLAN using the DHCPv6 Snooping binding table.
show tcam utilization detail	Displays additional TCAM usage information, such as application usage.
show capability profile	Displays the active and configured profile settings.

MIB Objects

```
alaCapManProfile
   alaCapManProfileTcamMode
```

capability trap-threshold

Configures the MAC and ARP table utilization high and low values for generating the associated traps.

capability trap-threshold {MAC | ARP} {HIGH *num* **| LOW** *num***}**

Syntax Definitions

MAC	Configures the MAC table threshold.
ARP	Configures the ARP table threshold.

Defaults

parameter	default
HIGH *num*	95
LOW *num*	90

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the table utilization reaches the configured HIGH value a trap will be sent indicating the usage has reached the HIGH value. The trap will continue to be periodically sent until the usage drops below the configured HIGH value.
- Once the usage drops to the configured LOW value a trap will be sent indicating the usage has dropped below the configured LOW value.
- The minimum LOW value is 5% and the maximum HIGH value is 95%. It is recommended to have a difference of at least 5% between LOW and HIGH values.

Examples

```
-> capability trap-threshold ARP HIGH 90 LOW 80
-> capability trap-threshold MAC HIGH 88 LOW 80
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show capability trap-threshold Displays the capability trap-threshold configured values.

MIB Objects

```
alaCapManTrapThreshold
   alaCapManTrapThresholdMacLow
   alaCapManTrapThresholdMacHigh
   alaCapManTrapThresholdArpLow
   alaCapManTrapThresholdArpHigh
```

license apply file

Activates the license for licensed protocols on the switch.

license apply {file *file_name* | **key** *license_key***}** [**order-id** *order_id*]

Syntax Definitions

file_name	The name of the license file containing the license keys.
license_key	Enter the individual license key. The license key can contain special characters, the key must encase using single quote character (").
order_id	The order ID for the MACsec license.

Defaults

By default, licensed protocols are not activated on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The license file can have any name.
- The license file is only used to activate the licensed features and does not need to remain on the switch.
- Using **key** option, the license key can be directly entered in the command. The license key can contain special characters; it is required to encase the key using single quote character ("). The **key** input is needed only for applying MACsec license.
- The switch must be rebooted to reflect the licensed feature set. For MACsSec and 10G license, a reboot is not required.
- A 10G license can be installed on the OmniSwitch 6560-24X4/P24X4/48X4/P48X4 models to upgrade ports 25/26 (24-port models) or ports 49/50 (48-port models) from 1G to 10G. There is no reboot required after applying this license, but the ports should be administratively disabled and re-enabled.
- The module type will continue to display as ‘U16L’ even after upgrading a ‘U16’ to a ‘U16E’.
- Order-id parameter is mandatory for MACsec license but it is not applicable for other licenses.
- The MACsec license is a site license and does not use the serial number and the MAC address of the switch. However, **order-id** is required for the license generator to generate MACsec license. The order ID value entered in this command is validated against the order ID in the license file. If this value does not match with the value stored in license file, MACsec license will not be installed.
- The order ID is a seven digit number and the license generation process appends the digit 0 at the beginning implicitly. Hence, it is required to provide eight digits (0 + 7 digits of the order ID) to install the license successfully.

Examples

```
-> license apply file /flash/swlicense.txt
```

```
The switch will reboot after the license is applied.
Are you sure you want to proceed(Y/N)?Y

-> license apply file \flash\swlicense.dat order-id "07766551"

-> license apply key 'hasJ-i{v!-[qVW-YPrt-t@YK' order-id "01234567"
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.1; **key** and **deactivate** parameters deprecated.
Release 8.6R1; MACsec site-wide license and OmniSwitch 6560 10-Gigabit port license support added.
Release 8.6R2; **key** parameter added.

Related Commands

show license-info	Displays all the licensed applications installed on the switch.

MIB Objects

```
alaCapManVcSwLicensingAction
   alaCapManVcSwLicensingActionArg
   alaCapManVcSwLicensingOrderId
```

show system

Displays basic system information for the switch. Information includes a user-defined system description, name, administrative contact, location, object ID, up time, and system services.

show system

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show system
System:
  Description:  Alcatel-Lucent Enterprise OS6900-X40 8.3.1.313.R01 GA, August 31,
2016.,
  Object ID:    1.3.6.1.4.1.6486.801.1.1.2.1.10.1.2,
  Up Time:      2 days 1 hours 32 minutes and 40 seconds,
  Contact:      Alcatel-Lucent, http://enterprise.alcatel-lucent.com,
  Name:         (none),
  Location:     Unknown,
  Services:     78,
  Date & Time:  FRI OCT 07 2016 14:10:02 (UTC)
Flash Space:
    Primary CMM:
      Available (bytes):  856936448,
      Comments         :  None
```

output definitions

System Description	The description for the current system. This description shows the current software version and the system date.
System Object ID	The SNMP object identifier for the switch.
System Up Time	The amount of time the switch has been running since the last system reboot.
System Contact	An user-defined administrative contact for the switch. This field is modified using the **system contact** command.
System Name	A user-defined text description for the switch. This field is modified using the **system name** command.

output definitions (continued)

System Location	The user-defined physical location of the switch. This field is modified using the **system location** command.
System Services	The number of current system services.
System Date & Time	The current system date and time. This field is modified using the **system date** and **system time** commands.
Flash Space: Primary CMM: Available (bytes)	The available flash memory space available on the *primary* management module of the switch.
Flash Space: Primary CMM: Comments	Comments regarding the available flash memory space available on the primary management module of the switch, if applicable.

Release History

Release 7.1.1; command introduced.

Related Commands

system contact	Specifies the administrative contact for the switch(for example, an individual or a department).
system name	Modifies the current system name of the switch.
system location	Specifies the current physical location of the switch.

MIB Objects

```
system
   systemContact
   systemName
   systemLocation
```

show hardware-info

Displays the current system hardware information. Includes CPU, flash, RAM, NVRAM battery, jumper positions, BootROM, and miniboot and FPGA information.

show hardware info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show hardware-info
CPU Type                          : PowerPC 8245,
Flash Manufacturer                : TOSHIBA,
Flash size                        : 67108864 bytes (64 MB),
RAM Manufacturer                  : (null),
RAM size                          : 268435456 bytes (256 MB),
NVRAM Battery OK ?                : YES,
BootROM Version                   : 6.1.2.20.R02 ,
Backup Miniboot Version           : 6.1.2.20.R02,
Default Miniboot Version          : 6.1.2.20.R02,
Product ID Register               : 54
Hardware Revision Register        : 00
CPLD Revision Register            : 06
XFP Module ID                     : 02
```

output definitions

CPU Type	The manufacturer and model number of the CPU used on the CMM.
Flash Manufacturer	The manufacturer of the flash memory used on the CMM.
Flash size	The total amount of flash memory (file space) on the CMM. This field specifies the total flash memory size only and does not indicate the amount of memory free or memory used.
RAM Manufacturer	The manufacturer of the RAM memory used on the CMM.
RAM size	The total amount of RAM memory on the CMM. This field specifies the total RAM memory only and does not indicate the amount of memory free or memory used.

output definitions (continued)

NVRAM Battery OK	The current status of the NVRAM battery. If the battery is OK, YES is displayed in this field. If the battery charge becomes low, NO is displayed in this field.
BootROM Version	The current BootROM version.
Backup Miniboot Version	The current backup miniboot version.
Default Miniboot Version	The current default miniboot version.
Product ID Register	The register number of the product ID.
Hardware Revision Register	The register number of the hardware revision.
CPLD Revision Register	The register number of the CPLD revision.
XFP Module ID	The ID number of the XFP module.

Release History

Release 7.1.1; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.
show cmm	Displays the basic hardware and status information for CMM modules running in the chassis.

MIB Objects

```
systemHardware
   systemHardwareBootCpuType
   systemHardwareFlashMfg
   systemHardwareFlashSize
   systemHardwareMemoryMfg
   systemHardwareMemorySize
   systemHardwareNVRAMBatteryLow
   systemHardwareJumperInterruptBoot
   systemHardwareJumperForceUartDefaults
   systemHardwareJumperRunExtendedMemoryDiagnostics
   systemHardwareJumperSpare
   systemHardwareBootRomVersion
   systemHardwareBackupMiniBootVersion
   systemHardwareDefaultMiniBootVersion
   systemHardwareFpgaVersionTable
   systemHardwareFpgaVersionEntry
   systemHardwareFpgaVersionIndex
```

show chassis

Displays the basic configuration and status information for the switch chassis.

show chassis

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show chassis
Local Chassis ID 1 (Master)
  Model Name:                   OS9900,
  Description:                  Chassis,
  Part Number:                  903722-90,
  Hardware Revision:            B,
  Serial Number:                T4720029,
  Manufacture Date:             Feb  1 2016,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Free Slots:                   4,
  Power Left:                   1540,
  Number Of Resets:             28,
  MAC Address:                  2c:fa:a2:13:e4:02
```

output definitions

Model Name	The factory-set model name for the switch. This field cannot be modified.
Description	The factory-set description for the switch. This field cannot be modified.
Part Number	The part number for the chassis.
Hardware Revision	The hardware revision level for the chassis.
Serial Number	The serial number for the chassis.
Manufacture Date	The date the chassis was manufactured.
Admin Status	The current power status of the chassis. Chassis information is obtained from a running CMM. Hence the value is always POWER ON.

output definitions (continued)

Operational Status	The current operational status of the chassis.
Free Slots	The number of free slots available for NIs.
Power Left	The power remaining for additional NIs.
Number of Resets	The number of times the CMM has been reset (reloaded or rebooted) since the last cold boot of the switch.
MAC Address	The base MAC address of the chassis.

Release History

Release 7.1.1; command introduced.

Related Commands

show hardware-info	Displays the current system hardware information.
show powersupply	Displays the hardware information and current status for chassis power supplies.
show fan	Displays the current operating status of chassis fans.

MIB Objects

```
chasChassisTable
   chasFreeSlots
   chasPowerLeft
```

show cmm

Displays basic hardware and status information for the CMM modules in a standalone switch.

show cmm [*slot***]**

Syntax Definitions

slot	Specifies the CMM by slot number or letter.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

On chassis-based switches, a CMM installed in the left CMM slot position is defined as CMM-A. A CMM installed in the right position is CMM-B.

Examples

```
-> show cmm
Chassis ID 1 Module in slot CMM-A
  Model Name:                     OS99-CMM,
  Module Type:                    0x7100101,
  Description:                    MGMT MODULE,
  Part Number:                    903754-90,
  Hardware Revision:              C06,
  Serial Number:                  U1820028,
  Manufacture Date:               May 10 2016,
  FPGA - Control:                 2.0.0,
  FPGA - Power:                   0.8,
  Admin Status:                   POWER ON,
  Operational Status:             UP,
  Max Power:                      64,
  CPU Model Type:                 Intel Atom C2518,
  MAC Address:                    2c:fa:a2:13:e4:02,
  Coreboot Version:               8.3.1.103.R01
```

output definitions

Model Name	The model name of the switch.
Model Type	A unique module ID specific to the type of module.
Description	A factory-defined description of the associated board.
Part Number	The part number for the board.
Hardware Revision	The hardware revision level for the board.
Serial Number	The serial number for the board.
Manufacture Date	The date the board was manufactured.

output definitions (continued)

FPGA - Control	FPGA version.
FPGA - Power	FPGA version
Admin Status	The current power status of the CMM. Information is obtained from a running CMM. Hence the value is always POWER ON.
Operational Status	The current operational status of the CMM.
Max Power	The maximum power for the CMM.
CPU Model Type	The CPU Model type.
MAC Address	The MAC address assigned to the chassis.
Coreboot Version	The boot version number for the CMM.

Release History

Release 7.1.1; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.
show slot	Displays the basic hardware and status information for Network Interface (NI) modules currently installed in the switch.
show module	Displays the basic information for either a specified module or all the modules installed in the chassis.
show module long	Displays the detailed information for either a specified module or all modules installed in the chassis.
show module status	Displays the basic status information for either a specified module or all modules installed in the chassis.
capability trap-threshold	Displays the status and configuration of Switch Fabric Modules (SFMs) on chassis-based switches.

MIB Objects

N/A

show slot

Displays the basic hardware and status information for Network Interface (NI) modules currently installed in the chassis.

show slot [*slot***]**

Syntax Definitions

slot	The slot number for a specific NI module installed in the chassis. If no slot number is specified, information for all the NI modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When this command is entered from the secondary CMM, the Operational and Admin Status for NIs will display as ‘UNKNOWN’.

Examples

```
-> show slot 1
Module in slot 1
  Model Name:                   OS10-GNI-C48,
  Description:                  10-1000 RJ45,
  Part Number:                  902434-90,
  Hardware Revision:            A07,
  Serial Number:                H03Q0008,
  Manufacture Date:             JAN 31 2007,
  FPGA - Physical 1:            007,
  Daughter FPGA - Physical 1:   002,
  Daughter FPGA - Physical 2:   002,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Consumption:            200,
  CPU Model Type   :            Motorola MPC854
  MAC Address:                  00:d0:95:01:04:
  ASIC - Physical 1:            BCM56620_A1,
  ASIC - Physical 2:            BCM56620_A1,
  ASIC - Physical 3:            BCM56620_A1,
  ASIC - Physical 4:            BCM56620_A1,
  ASIC - Physical 5:            BCM56620_A1,
  ASIC - Physical 6:            BCM56620_A1,
  UBOOT Version:                7.1.1.412.R01,
```

output definitions

Model Name	The NI module name. For example, OS9-GNI-C24 indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Description	A general description of the NI. For example, 24pt 10/100/1000BaseT Mod indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Part Number	The part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The serial number for the NI printed circuit board (PCB).
Manufacture Date	The date the NI was manufactured.
FPGA/Daughter FPGA	The FPGA versions.
Admin Status	The current power status of the NI. Options include POWER ON or POWER OFF.
Operational Status	The operational status of the NI. Options include UP or DOWN. The operational status can be DOWN while the power status is on, indicating a possible software issue.
Power Consumption	The current power consumption for the module.
CPU Model Type	The CPU model type.
MAC Address	The MAC address assigned to the NI.
ASIC - Physical	General information regarding the NI module ASICs.
UBOOT Version	UBOOT version of the NI.

Release History

Release 7.1.1; command introduced.

Related Commands

reload slot	Reloads the specified NI module.
power slot	Turns the power on or off for a specified Network Interface (NI) module.
show module	Displays the basic information for either a specified module or all modules installed in the chassis.
show module long	Displays the detailed information for either a specified module or all modules installed in the chassis.
show module status	Displays the basic status information for either a specified module or all modules installed in the chassis.

MIB Objects

```
chasEntPhysOperStatus
```

show module

Displays the basic information for either a specified module or all modules installed in a standalone switch chassis.

show module [*slot*]

Syntax Definitions

slot	The slot number or CMM letter for a specific module installed in the chassis. If no slot number is specified, information for all modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show module
                                      HW    Mfg
Slot     Part-Number     Serial #    Rev   Date       Model Name
-------+--------------+------------+---+-----------+---------------------------
CMM-A    902271-10      E23L9059     002 JUN 08 2004  OS10-CPM
SLOT-1   902271-10      E23L9059     002 JUN 08 2004  OS10-GNI-C48
```

output definitions

Slot	The chassis slot position of the module.
Part-Number	The part number for the module.
Serial #	The serial number for the module.
Rev	The hardware revision level for the module.
Date	The date the module was manufactured.
Model Name	The descriptive name for the module.

Release History

Release 7.1.1; command introduced.

Related Commands

show module long	Displays the detailed information for either a specified module or all modules installed in the chassis.
show module status	Displays the basic status information for either a specified module or all modules installed in the chassis.

MIB Objects

N/A

show module long

Displays the detailed information for either a specified module or all the modules installed in a standalone switch chassis.

show module long [*slot***]**

Syntax Definitions

slot	The slot number or CMM letter for a specific module installed in the chassis. If no slot number is specified, information for all modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show module long 1
Module in slot 1
  Model Name:                   OS99-GNI-P48,
  Module Type:                  0x70e2101
  Description:                  48 G POE,
  Part Number:                  903726-90,
  Hardware Revision:            A07,
  Serial Number:                H03Q0008,
  Manufacture Date:             JAN 31 2007,
  FPGA - Control                1.2.4,
  FPGA - Power                  0.9
  Daughter FPGA - Physical 1:   002,
  Daughter FPGA - Physical 2:   002,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Max Power:                    54,
  CPU Model Type   :            Intel Atom C2338
  MAC Address:                  00:d0:95:01:04:
  ASIC - Physical 1:            BCM56620_A1,
  ASIC - Physical 2:            BCM56620_A1,
  ASIC - Physical 3:            BCM56620_A1,
  ASIC - Physical 4:            BCM56620_A1,
  ASIC - Physical 5:            BCM56620_A1,
  ASIC - Physical 6:            BCM56620_A1,
  UBOOT Version:                7.1.1.412.R01,
  POE-Software Version:         PD69100 Software Version 00.0255.01 Hardware
                                Version 00 NI 1,
```

output definitions

Model Name	The NI module name.
Description	A general description of the NI.
Part Number	The part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The serial number for the NI printed circuit board (PCB).
Manufacture Date	The date the NI was manufactured.
FPGA/Daughter FPGA	The FPGA versions.
Admin Status	The current power status of the module. Options include POWER ON or POWER OFF.
Operational Status	The operational status of the module. Options include UP or DOWN. The operational status can be DOWN while the power status is on, indicating a possible software issue.
Max Power	The maximum power consumption for the module.
CPU Model Type	The CPU model type.
MAC Address	The MAC address assigned to the module.
ASIC - Physical	General information regarding the module ASICs.
UBOOT Version	UBOOT version of the module.
POE-Software Version	The PoE controller firmware/hardware revision.

Release History

Release 7.1.1; command introduced.

Related Commands

show module	Displays the basic information for either a specified module or all modules installed in the chassis.
show module status	Displays the basic status information for either a specified module or all modules installed in the chassis.

MIB Objects

N/A

show module status

Displays the basic status information for either a specified module or all modules installed in a standalone switch chassis.

show module status [*slot***]**

Syntax Definitions

slot	The slot number or CMM letter for a specific module installed in the chassis. If no slot number is specified, information for all modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When this command is entered from the secondary CMM, the Operational and Admin Status for NIs will display as 'UNKNOWN'.

Examples

```
-> show module status
       Operational                Firmware
Slot     Status      Admin-Status   Rev           MAC
------+-------------+------------+---------+-----------------
CMM-A    UP           POWER ON      N/A     00:d0:95:a3:e5:09
SLOT-1   UP           POWER ON      N/A     00:d0:95:a3:e5:0b
```

output definitions

Slot	The chassis slot position of the module. For detailed slot numbering information, refer to the "Chassis and Power Supplies" chapter of the *Hardware User Guide*. Refer to page 58-37 for additional information on CMM callouts.
Operational Status	The operational status of the module. Options include UP or DOWN. For NI and secondary CMM modules, the operational status can be DOWN while the power status is on, indicating a possible software issue.
Admin-Status	The current power status of the module. Options include POWER ON or POWER OFF.
Firmware Rev	The firmware version for module ASICs.
MAC	For the CMM, the base chassis MAC address is displayed. For NI modules, the MAC address for the corresponding NI is displayed.

Release History

Release 7.1.1; command introduced.

Related Commands

show module	Displays the basic information for either a specified module or all the modules installed in the chassis.
show module long	Displays the detailed information for either a specified module or all the modules installed in the chassis.

MIB Objects

N/A

show powersupply

Displays the hardware information and current status for chassis power supplies.

show powersupply [*slot***]**

Syntax Definitions

slot	The slot number for a specific power supply installed in the chassis. If no power supply number is specified, information for all power supplies is displayed.
powersave status	Displays the status of the power saving functionality.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show powersupply
           Total     Power    Input     PS
Slot  PS   Power     Used     Voltage   Type     Status   Location
----+----+---------+--------+---------+--------+--------+----------
      1     2400      0        0         AC       UP       Internal
      2     2400      0        0         AC       UNPLUG   Internal
      3     2400      564      226       AC       UP       Internal
      4     2400      504      226       AC       UP       Internal
      5     --        --       --        --       --       --
      6     --        --       --        --       --       --
      7     --        --       --        --       --       --
      8     --        --       --        --       --       --

-> show powersupply
           Total     Power    PS
Slot  PS   Power     Used     Type     Status      Location    Airflow
----+----+---------+--------+--------+-----------+-----------+-----------
      1     450       201      AC       UP         Internal    Front to Rear
      2     450       50       AC       UP         Internal    Front to Rear
```

```
-> show powersupply 1

Module in slot PS-1
 Model Name:                     YM-2451DDR,
 Module Type:                    DC/DC Power Supply, Front to Rear Airflow
 Description:                    OS-PS-450W-D
 Hardware Revision:              B0,
 Serial Number:                  1020000417,
 Manufacture Date:               May 14 2010,
 Operational Status:             UP,
 Power Provision:                450W
```

output definitions

Model Name	The power supply model number.
Description	A description of the associated power supply. This field reflects the model name in most cases.
Part Number	The part number for the power supply.
Hardware Revision	The hardware revision level for the power supply.
Serial Number	The serial number for the power supply.
Manufacture Date	The date the power supply was manufactured.
Operational Status	The operational status of the power supply. Options include UP or DOWN.
Power Provision	The number of watts provided by this power supply.
PS	The slot number of the power supply.
Total Power	The number of watts provided by this power supply.
Power Used	The number of watts being used by this power supply.
Input Voltage	The input line voltage of this power supply.
PS type	The type of power supply. AC or DC.
Operational Status	The operational status of the power supply. Options include UP, DOWN, or UNPLUG.
Location	The location of the power supply. Options include Internal or External. Slots 5-8 are for the optional power shelf.
Airflow	Direction of airflow.

Release History

Release 7.1.1; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.

MIB Objects

N/A

show fan

Displays the current operating status of chassis fans.

show fan [*slot***]**

Syntax Definitions

slot	Specifies the slot number of the fantray.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guideline

N/A

Examples

```
-> show fan
Chassis Fan  Status
-------+---+-----------
   1     1   Running
   1     2   Running
   1     3   Running
   1     4   Not Running
```

output definitions

Chassis/Tray	The chassis/tray ID.
Fan	The fan number describing the fan position.
Status/Functional	The current operational status of the corresponding fan.
Speed	The speed of the fan.
Airflow	-

Release History

Release 7.1.1; command introduced.

Related Commands

show fantray	Displays the current operating status of chassis fantrays.

MIB Objects

N/A

show fantray

Displays the current operating status of chassis fantrays.

show fantray [*slot***]**

Syntax Definitions

slot	Specifies the slot number of the fantray.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guideline

N/A

Examples

```
-> show fantray
              | Working |  Fan
Tray | Status |  Fans   | Load %
-----+--------+---------+--------
  1     ON         4        50
```

output definitions

Chassis/Tray	The chassis/Tray ID.
Status	The current operational status of the fantray.
Working Fans	The number of working fans.
Fan Load %	The load of the fantray.

Release History

Release 7.1.1; command introduced.

Related Commands

show fantray	Displays the current operating status of chassis fantrays.

MIB Objects

```
N/A
```

show temperature

Displays the internal operating temperature of the chassis, as well as current temperature threshold settings.

show temperature [fabric [*index***] | slot [***index***] | fantray [***index***] | cmm [***index* | *cmm_letter***] | chassis-id** *chassis***]**

Syntax Definitions

index	Specifies the index number.
cmm_letter	Specifies the CMM letter.
chassis	The ID number of the chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command displays the internal operating temperature, not the ambient temperature, of the current operating chassis as well as current temperature threshold settings.
- Refer to the appropriate *Hardware Users Guide* for detailed information about temperature thresholds for a specific OmniSwitch model.

Examples

```
-> show temperature
Chassis/Device | Current |  Range  |  Danger | Thresh |  Status
---------------+---------+---------+---------+--------+-----------------
 1/CMMA            48     -45 to 93      98       93     UNDER THRESHOLD
```

output definitions

Chassis/Device	The device being measured (CMM, Fabric, or NI)
Current	The current CPU temperature in Celsius.
Range	The supported threshold range.
Danger	The danger threshold value. This value is based on the switch model and is not configurable.
Thresh	The warning temperature threshold, in degrees Celsius. If the switch reaches or exceeds this temperature, the primary switch or CMM TEMP LED displays amber and a warning is sent to the user.
Status	Whether the current temperature has reached the threshold.

Release History

Release 7.1.1; command introduced.

Related Commands

show fan	Shows the hardware information and current status for the chassis fans.

MIB Objects

```
chasChassisTable
   chasHardwareBoardTemp
   chasHardwareCpuTemp
   chasTempRange
   chasTempThreshold
   chasDangerTempThreshold
```

show hash-control

Displays the current hash control settings for the switch.

show hash-control [non-ucast]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

N/A

Examples

```
-> show hash-control
Hash Mode    = brief,
Udp-Tcp-Port = disabled

-> show hash-control non-ucast
Hash Status = Enabled,
Hash Mode : Normal
```

output definitions

Hash Mode	The current Hash Mode.
Udp-Tcp-Port	Status of UDP/TCP hashing.
Non-ucast Hash Status	Status of Non-ucast Hash status.

Release History

Release 7.2.1; command introduced.

Related Commands

powersupply type	Configures the hash mode of the switch.

MIB Objects

```
alaChasHashMode
alaChasUdpTcpPortMode
alachasNonUCHashControl
```

show license-info

Displays all the licensed applications installed on the switch.

show license-info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to verify which licenses are installed on the switch.
- The number of days remaining is only applicable for demo licenses.
- The module type will continue to display as ‘U16L’ even after upgrading a ‘U16’ to a ‘U16E’.

Examples

```
-> show license-info
                                                Time (Days)     Upgrade        Expiration
VC   device   License            Type          Remaining       Status         Date
----+------+--------------+--------------+--------------+--------------+----------------
3       0    Advanced           PERM            NA             NA             NA
3       0    10G                PERM            NA             NA             NA
4       0    Advanced           PERM            NA             NA             NA
4       0    10G                PERM            NA             NA             NA
5       0    Advanced           PERM            NA             NA             NA
5       0    10G                PERM            NA             NA             NA
6       0    Advanced           PERM            NA             NA             NA
6       0    10G                PERM            NA             NA             NA
```

output definitions

VC	Virtual chassis identifier.
Device	Slot number of NI.
License	Displays the feature license installed on the switch. Advanced, Data Center, U16L
Type	The type of license: Demo or Permanent.
Time (Days) Remaining	Time of days remaining for a demo license. Display as ‘NA’ for permanent licenses.
Upgrade Status	Status of the upgrade.
Expiration Date	Date of license expiry.

Release History

Release 7.2.1; command was introduced.
Release 8.6R1; **Upgrade Status** and **Expiration Date** fields added.

Related Commands

license apply file	Activates the license for licensed protocols on the switch.

MIB Objects

```
alaVcCapManSwLicensingInfoTable
   alaVcLicensedvcSlot
   alaVcLicensedMask
   alaVcLicenseType
   alaVcTimeRemain
```

show bluetooth status

Displays the current USB adapter with Bluetooth technology configuration.

show bluetooth status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guideline

N/A

Examples

```
-> show bluetooth status
Admin Status       : disabled,
Transmit Power     : low,

Chassis      Operational Status
----------+--------------------------
 1          Not Present
```

output definitions

Admin Status	Whether the USB adapter with Bluetooth technology is enabled or disabled.
Transmit Power	Whether transmit power is high or low.
Chassis	The chassis identifier.
Operational Status	notPresent - No USB adapter with Bluetooth technology present. connectionInactive - USB adapter with Bluetooth technology present but inactive. connectionActive - USB adapter with Bluetooth technology present and active.

Release History

Release 8.1.1; command introduced.

Related Commands

bluetooth	Enables or disables a USB adapter with Bluetooth technology and configures the power level.

MIB Objects

N/A

show me

Executes an LED blink pattern for 10 seconds that is used by the USB adapter with Bluetooth technology to identify the connected switch.

show me

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, OmniSwitch 6900-V72, 6900-C32

Usage Guideline

Use this command in a virtual chassis to identify which switch currently has USB adapter with Bluetooth technology connectivity.

Examples

```
-> show me
The Chassis ID LED will blink for 10 seconds.
```

Release History

Release 8.1.1; command introduced.

Related Commands

bluetooth	Enables or disables a USB adapter with Bluetooth technology and configures the power level.

MIB Objects

N/A

show tcam utilization

Displays runtime information about the Ternary Content Addressable Memory (TCAM) utilization for each stage of each TCAM on each slot of the switch.

show tcam utilization [*chasiss/slot***] [***chasiss/slot/tcam***]**

Syntax Definitions

chassis/slot	A chassis ID and slot number. Use this parameter to display TCAM utilization for a specific slot.
chasiss/slot/tcam	A chassis ID, slot, and TCAM number. Use this parameter to display utilization for a specific TCAM.

Defaults

By default, TCAM utilization is displayed for the entire switch.

Platforms Supported

OmniSwitch 6465, 6560, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- The utilization is represented in terms of the minimum-sized entry supported by the TCAM.
- This command replaces the **show qos slice** command on the supported OmniSwitch platforms listed above; the **show qos slice** command, however, is still available on the other OmniSwitch platforms.

Examples

```
-> show tcam utilization

Legend:
 C/S/T = Chassis/Slot/TCAM
 PI = Pre-Ingress
 I  = Ingress
 E  = Egress

                 Min-    Reserved      Total
 C/S/T   Stage  entry-   min-key-    min-key-      Utilization
                 size     entries     entries       percentage
-----------------------------------------------------------------
 1/1/1    PI      10       8448       12288            68%
 1/1/1     I      10       9924       18432            53%
 1/1/1     E      10        768        6144            12%
 1/3/1    PI      10       8448       12288            68%
 1/3/1     I      10       9924       18432            53%
 1/3/1     E      10        768        6144            12%
 1/3/2    PI      10       8448       12288            68%
 1/3/2     I      10       9924       18432            53%
 1/3/2     E      10        768        6144            12%
 1/3/3    PI      10       8448       12288            68%
 1/3/3     I      10       9924       18432            53%
```

```
 1/3/3     E      10        768        6144            12%
 1/3/4    PI      10       8448       12288            68%
 1/3/4     I      10       9924       18432            53%
 1/3/4     E      10        768        6144            12%
 1/3/5    PI      10       8448       12288            68%
 1/3/5     I      10       9924       18432            53%
 1/3/5     E      10        768        6144            12%
 1/3/6    PI      10       8448       12288            68%
 1/3/6     I      10       9924       18432            53%
 1/3/6     E      10        768        6144            12%
 1/4/1    PI      10       8448       12288            68%
 1/4/1     I      10      16068       23040            69%
 1/4/1     E      10        768        1536            50%

-> show tcam utilization 1/4

Legend:
 C/S/T = Chassis/Slot/TCAM
 PI = Pre-Ingress
 I  = Ingress
 E  = Egress

                 Min-    Reserved      Total
 C/S/T   Stage  entry-   min-key-    min-key-      Utilization
                 size     entries     entries       percentage
-----------------------------------------------------------------
 1/4/1    PI      10       8448       12288            68%
 1/4/1     I      10      16068       23040            69%
 1/4/1     E      10        768        1536            50%
```

Release History

Release 8.3.1; command introduced.

Related Commands

show tcam utilization detail Displays additional TCAM usage information, such as application usage.

MIB Objects

```
alaTcamUtilTable
   alaTcamChassis
   alaTcamSlot
   alaTcamIndex
   alaTcamStage
   alaTcamEntrySize
   alaTcamUsedEntries
   alaTcamTotalEntries
   alaTcamPercentUsed
```

show tcam utilization detail

Displays the Ternary Content Addressable Memory (TCAM) utilization of each application (or application group) for each stage of each TCAM on each slot of the switch.

show tcam utilization [*chasiss/slot***] [***chasiss/slot/tcam***] detail**

Syntax Definitions

chassis/slot	A chassis ID and slot number. Use this parameter to display TCAM utilization for a specific slot.
chasiss/slot/tcam	A chassis ID, slot, and TCAM number. Use this parameter to display utilization for a specific TCAM.

Defaults

By default, the detailed TCAM utilization is displayed for the entire switch.

Platforms Supported

OmniSwitch 6465, 6560, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

The utilization is represented in terms of the minimum-sized entry supported by the TCAM.

Examples

```
-> show tcam utilization detail

Legend:
 C/S/T = Chassis/Slot/TCAM
 PI = Pre-Ingress
 I  = Ingress
 E  = Egress

        App       App     Resource                          Entry
C/S/T   Group     Name      Name                     Stage   Size    Used   Reserved Available
        Name                                                      Entries  Entries  Entries
-------------------------------------------------------------------------------------------
 1/1/1 SYSPRE      -      System PreIngress           PI     30      48       256      208
 1/1/1 TTI         -      System TTI                  PI     30       0      2048     2048
 1/1/1 TUNNEL_SVC  -      Tunnel Services PreIngress  PI     30       0       512      512
 1/1/1 SYSHI       -      System High                  I     30     134       256      122
 1/1/1 SYSLO       -      System Low                   I     60      76       256      180
 1/1/1 TUNNEL_SVC  -      Tunnel Services Ingress      I     10       0      2052     2052
 1/1/1 -           QOS                                 I     60       0       512      512
 1/1/1 -           UDPRLY UDP_RLY_ISF                  I     60       0       256      256
 1/1/1 -           ETHOAM                              I     30       0        64       64
 1/1/1 -           PVLAN  PVLAN1                       I     30       0       256      256
 1/1/1 -           PVLAN  PVLAN2                       E     30       0       256      256
 1/3/1 SYSPRE      System PreIngress                  PI     30      48       256      208
 1/3/1 TTI         -      System TTI                  PI     30       0      2048     2048
 1/3/1 TUNNEL_SVC  -      Tunnel Services PreIngress  PI     30       0       512      512
 1/3/1 SYSHI       -      System High                  I     30     134       256      122
 1/3/1 SYSLO       -      System Low                   I     60      76       256      180
 1/3/1 TUNNEL_SVC  -      Tunnel Services Ingress      I     10       0      2052     2052
```

```
 1/3/1 -           QOS                              I     60       0       512      512
 1/3/1 -           UDPRLY UDP_RLY_ISF               I     60       0       256      256
 1/3/1 -           ETHOAM                           I     30       0        64       64
 1/3/1 -           PVLAN  PVLAN1                    I     30       0       256      256
 1/3/1 -           PVLAN  PVLAN2                    E     30       0       256      256
 1/4/1 SYSPRE      -      System PreIngress         PI     30      48       256      208
 1/4/1 TTI         -      System TTI                PI     30       0      2048     2048
 1/4/1 TUNNEL_SVC  -      Tunnel Services PreIngress PI    30       0       512      512
 1/4/1 SYSHI       -      System High               I     60     134       256      122
 1/4/1 SYSLO       -      System Low                I     60      76       256      180
 1/4/1 TUNNEL_SVC  -      Tunnel Services Ingress   I     10       0      2052     2052
 1/4/1 -           QOS                              I    120       0       512      512
 1/4/1 -           UDPRLY UDP_RLY_ISF               I    120       0       256      256
 1/4/1 -           ETHOAM                           I     30       0        64       64
 1/4/1 -           PVLAN  PVLAN1                    I     60       0       256      256
 1/4/1 -           PVLAN  PVLAN2                    E     30       0       256      256

-> show tcam utilization 1/4/1 detail

Legend:
 C/S/T = Chassis/Slot/TCAM
 PI = Pre-Ingress
 I  = Ingress
 E  = Egress

        App       App     Resource                          Entry
C/S/T   Group     Name      Name                    Stage   Size    Used    Reserved Available
        Name                                                      Entries  Entries  Entries
-------------------------------------------------------------------------------------------
 1/4/1 SYSPRE      -      System PreIngress         PI     30      48       256      208
 1/4/1 TTI         -      System TTI                PI     30       0      2048     2048
 1/4/1 TUNNEL_SVC  -      Tunnel Services PreIngress PI    30       0       512      512
 1/4/1 SYSHI       -      System High               I     60     134       256      122
 1/4/1 SYSLO       -      System Low                I     60      76       256      180
 1/4/1 TUNNEL_SVC  -      Tunnel Services Ingress   I     10       0      2052     2052
 1/4/1 -           QOS                              I    120       0       512      512
 1/4/1 -           UDPRLY UDP_RLY_ISF               I    120       0       256      256
 1/4/1 -           ETHOAM                           I     30       0        64       64
 1/4/1 -           PVLAN  PVLAN1                    I     60       0       256      256
 1/4/1 -           PVLAN  PVLAN2                    E     30       0       256      256
```

Release History

Release 8.3.1; command introduced.

Related Commands

show tcam utilization	Displays runtime information about the TCAM utilization.
show tcam app-groups	Displays the application groups and the applications that belong to each group within the context of TCAM utilization

MIB Objects

```
alaTcamDetailedUtilTable
   alaTcamDTableChassis
   alaTcamDTableSlot
   alaTcamDTableTCAMIndex
   alaTcamDTableStage
   alaTcamDTableGResourceId
   alaTcamDTableEntrySize
   alaTcamDTableUsedEntries
   alaTcamDTableReservedEntries
   alaTcamDTableAvailableEntries
   alaTcamDTableAppGroupName
   alaTcamDTableAppName
   alaTcamDTableResourceName
```

show tcam app-groups

Displays the application groups and the applications that belong to each group within the context of Ternary Content Addressable Memory (TCAM) utilization.

show tcam app-groups

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show tcam app-groups
    App-Group Name                   App Name
---------------------------------+------------------------
 SYSPRE                          -
 SYSHI                           -
 SYSLO                           -
 TTI                             -
 TUNNEL_SVC                      -
 TUNNEL_SVC                      -
 SYSEGR                          -
 EGR_SVC_PORT                    -
 -                               IPV6
 -                               QOS
 -                               PVLAN
 -                               PVLAN
 -                               AG
```

Release History

Release 8.3.1; command introduced.

Related Commands

show tcam utilization detail	Displays additional TCAM usage information, such as application usage.
show tcam utilization	Displays runtime information about the TCAM utilization.

MIB Objects

```
alaTcamDetailedUtilTable
   alaTcamDTableChassis
   alaTcamDTableSlot
   alaTcamDTableTCAMIndex
   alaTcamDTableAppGroupName
   alaTcamDTableAppName
```

show capability profile

Displays the active and configured profile settings.

show capability profile

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6560, OmniSwitch 6900-V72, 6900-C32, OmniSwitch 6900-X72

Usage Guidelines

- The switch must be rebooted for the configured profile to take effect.
- On the OmniSwitch 6900-V72, 6900-C32, and OmniSwitch 6900-X72, this command displays the configured and active mode to indicate if the switch is operating in the router or switch mode. The configured mode is changed using the **capability profile** command.
- On the OmniSwitch 6560, this command displays the configured and active TCAM mode (source or destination IPv6 filtering). The configured TCAM mode is changed using the **capability profile tcam mode** command.

Examples

Sample output on the OmniSwitch 6900-V72, 6900-C32, and OmniSwitch 6900-X72:

```
-> show capability profile
Configured  Profile :      Router
Active  Profile     :      Switch
```

Sample output on the OmniSwitch 6560:

```
-> show capability profile
Configured  TCAM Mode :      dest-ipv6
Active  TCAM mode     :      dest-ipv6
```

Release History

Release 8.5R2; command introduced.
Release 8.6R1; TCAM mode display added.

Related Commands

capability profile	Configures the mode of the switch to be either switch or router.
capability profile tcam mode	Configures the source IPv6 filtering or destination IPv6 filtering TCAM mode for the switch.

MIB Objects

```
alaCapManProfile
   alaCapManProfileMode
alaCapManProfile
   alaCapManProfileTcamMode
```

show pmd-files

Displays a list of PMD files generated on the switch.

show pmd-files

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show pmd-files

########### PMD files(Chassis 1 /flash/pmd) ##########

pmd-capmanc-06.10.2014-15.24.49
pmd-agCmm-01.21.2016-15.07.32
pmd-agCmm-01.21.2016-15.08.09
pmd-capmanc-07.23.2016-14.28.25
pmd-07.23.2016-14.39.24
pmd-capmanc-2016.07.23-14.42.42p
pmd-bcd2-07.13.2017-11.22.28
pmd-bcd2-2017.07.26-15.02.12p

8 PMD files found
```

Release History

Release 8.4.1.R03; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.

MIB Objects

N/A

show capability trap-threshold

Displays the capability trap-threshold configured values.

show capability trap-threshold

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the configured High and Low trap-threshold table utilization values.

Examples

```
-> show capability trap-threshold
 Name       High    Low
----------+------+-------
MAC           95     90
ARP           95     90
```

Release History

Release 8.6R1; command introduced.

Related Commands

capability trap-threshold	Configures the MAC and ARP table utilization high and low values for generating the associated traps.

MIB Objects

```
alaCapManTrapThreshold
   alaCapManTrapThresholdMacLow
   alaCapManTrapThresholdMacHigh
   alaCapManTrapThresholdArpLow
   alaCapManTrapThresholdArpHigh
```

show tech-support

Creates a log or tar file gathering important switch information that can be used by technical support.

show tech-support [layer2 | layer3 | eng [complete]]

Syntax Definitions

layer2	Gathers layer 2 switch configuration information.
layer3	Gathers layer 3 switch configuration information.
eng [complete]	Gathers all relevant switch information from flash such as log files, configuration files, directories and creates an archive file with all the information.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Running the command with no parameters creates a **tech_support.log** file.
- The **layer2** parameter creates a **tech_support_layer2.log** file.
- The **layer3** parameter creates a **tech_support_layer3.log** file.
- The **eng** parameter creates a **tech_support_eng.tar** file. The **complete** parameter creates a **tech_support_complete.tar** file with information from all switches in a VC along with the log files.

Examples

```
-> show tech-support
-> show tech-support layer2
-> show tech-support layer3
-> show tech-support eng
-> show tech-support eng complete
```

Release History

Release 7.3.4.R02; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.

MIB Objects

N/A

security key-chain gen-random-key

Generates a 32-byte random key.

security key-chain gen-random-key

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, 9900

Usage Guidelines

The generated key can be used as an input value for hex-key or encrypt-key while creating a security key.

Examples

```
-> security key-chain gen-random-key
0x0102030405060708090A0B0C0D0E0F
```

Release History

Release 8.4.1 R03; command introduced.

Related Commands

security key	This command creates an authentication key into the system.

MIB Objects

N/A

security key

Creates an authentication key into the system.

security key *key_id* **algorithm {sha256 {encrypt-key** *encrypt_key* **| key** *simple_key***} start-time** *mm/dd/yyyy* **[***hh:mm***] [lifetime** *days* **[***hh:mm***]] | aes-gcm-128 {hex-key** *hex_key* **| encrypt-key {***hex* **|** *num***}} | aes-cmac-128 {hex-key** *hex_key* **| encrypt-key {***hex* **|** *num***}} keyed-name** *hex-kn***}**

no security key *key_id* [*-key_id2***]**

Syntax Definitions

key_id	The key ID. This can be in the range 1-256.
sha256	Specifies that the SHA256 authentication algorithm is used as authentication key.
encrypt_key	The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form. The key can range from 16 to 512 characters in length.
simple_key	Key will be plain text ASCII up to 118 characters. Use quotes ("") around the string if the key contains multiple words with spaces between them. Plain text key can range from 16 to 118 characters in length.
mm/dd/yyyy	Key activation time. Granularity is up to minutes. Enter the start time in the format mm/dd/yyyy hh:mm where mm is the month, dd is the day, yyyy is the year, hh is the hour, mm is the minutes. For example, 08/08/2005 14:30
days	Validity duration of the key in terms of days and time. Lifetime can be in the range 1 - 9125 days.
aes-gcm-128	Specifies that the aes-gcm-128 authentication algorithm is used as authentication key.
aes-cmac-128	Specifies that the aes-cmac-128 authentication algorithm is used as authentication key.
hex-key *hex_key*	The key value in hexadecimal format (0xhex) for aes-gcm-128 or aes-cmac-128 algorithm. Configuration snapshot displays the authentication key in the encrypted form. The key can range from 1 to 32 characters in length (16 byte).
encrpt-key *hex*	The key in hexadecimal format for aes-gcm-128 or aes-cmac-128 algorithm. The key can range from 1 to 32 characters in length (16 byte).
encrpt-key *num*	The key in numerical format for aes-gcm-128 or aes-cmac-128 algorithm. The key can range from 1 to 32 characters in length (16 byte).
hex-kn	The Connectivity Association Key Name (CKN) value in hexadecimal format (0xhex). The key name can range from 1 to 64 characters in length (32 byte).

Defaults

parameter	default
lifetime *days*	180 days

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, 9900

Usage Guidelines

- The switch can have a maximum of 256 keys.
- Current active key is determined based on the lowest numerical key ID. When the current active key expires, if the keychain has multiple active keys, the switch will switchover to active key having lowest key ID.
- When the current active key expires, if the keychain does not have any other active key, the switch will bring down all the adjacencies formed using that keychain.
- Parameters of a key can be modified if the key is not in use. Once the key is attached to any of the keychains, no more modification is allowed.
- Use the **no** form of this command to delete a key.
- To delete a key, first disassociate the keychain from a user application, and detach the key from the keychain.
- The show commands will always display the key-string in an encrypted format.
- Use the command **security key-chain gen-random-key** to generate a the hex-key to be configured for the aes-gcm-128 or aes-cmac-128 algorithm.
- For aes-gcm-128 or aes-cmac-128 algorithm, the key value in hexadecimal format (hash-key or encrypt-key) can range from 1 to 32 characters in length. For key size greater than 32 characters, an error message is displayed. Any key size lesser than 16 byte is accepted and preceded with 0s to make it 32 characters.
- For aes-cmac-128 algorithm, the length of the key name in hexadecimal format can range from 1 to 64 characters in length. For key name size greater than 64 characters, an error message is displayed. Any key name size lesser than 64 characters is accepted and preceded with 0s to make it 64 characters.
- A keychain using the aes-gcm-128 authentication algorithm must be attached only to MACsec interface for its static-SAK configured under MACsec mode "static" only.
- A keychain using the aes-cmac-128 authentication algorithm must be attached only to MACsec interface for its Static Connectivity Association Key (static-CAK) using Pre-Shared key configured under MACsec mode "dynamic" only.

Examples

```
-> security key 5 algorithm sha256 key "passwordstring123" start-time 1/31/2017
00:00 life-time 180 10:30
-> security key 5 algorithm sha256 key "passwordstring123" start-time 5/2/2017
life-time 150
-> security key 1 algorithm aes-gcm-128 hex-key 0x0102030405060708090A0B0C0D0E0F
```

```
-> security key 1 algorithm aes-cmac-128 hex-key 0x0102030405060708090A0B0C0D0E0F
keyed-name 0x0102030405060708090A0B0C0D0FFF

-> no security key 5
```

Release History

Release 8.4.1; command introduced.
Release 8.4.1 R03; **aes-gcm-128** keyword added.
Release 8.5R2; **aes-cmac-128** keyword added.

Related Commands

show security key	This command displays the configured keys in the system.

MIB Objects

```
alaSecKeyIdalaSecKeyAlgorithm
alaSecKeyType
alaSecKeyAuthKey
alaSecKeyStartTime
alaSecKeyLifeTime
alaSecKeyRowStatus
```

security key-chain

This command creates a system level security keychain.

security key-chain *key_chain_id* **[name** *key_chain_name***]**

no security key-chain *key_chain_id1* **[-***key_chain_id2***]**

Syntax Definitions

key_chain_id	The keychain ID. This can be in the range 1-32.
key_chain_name	The keychain name. The keychain name can range from 1 to 16 characters in length.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, 9900

Usage Guidelines

- There can be a maximum of 32 keychains in the device, and each of them can hold multiple keys of the same algorithm type.
- Use the **no** form of this command to delete a keychain.
- To delete a keychain, first disassociate the keychain from the user application.
- Deleting a keychain will not delete the keys associated with the keychain. Keys will subsequently remain configured, but will not be associated to any keychain, until reassociation.
- The keychain ID is associated to user applications such as ISIS, OSPF. The authentication information is carried in the Hello packet. If the authentication succeeds, then adjacency is formed. The two remote machines should have same current key ID and same authentication type.
- Changing the switch system clock impacts the status of the keys.

Examples

```
-> security key-chain 1 globalKeyChain
-> no security key-chain 1-3
-> no security key-chain 4
```

Release History

Release 8.4.1; command introduced.

Related Commands

show security key-chain	This command displays the configured keychains in the system.

MIB Objects

```
alaSecKeyChainId
alasecKeyChainName
```

security key-chain key

This command associates a key into the specified keychain.

security key-chain *key_chain_id* **key** *key_id* [*-key_id2*]

no security key-chain *key_chain_id1* **[**-*key_chain_id2*]}

Syntax Definitions

key_chain_id	The keychain ID.
key_id	The key ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, 9900

Usage Guidelines

- A keychain can be configured with multiple keys of the same algorithm type.
- Use the **no** form of this command to disassociate a key from a security keychain.
- To disassociate a key from the keychain, first disassociate the keychain from the user application, and detach the key from the keychain.

Examples

```
-> security key-chain 1 key 5
-> no security key-chain 1
```

Release History

Release 8.4.1; command introduced.

Related Commands

security key-chain	This command creates a system level security keychain.
security key	This command creates an authentication key into the system.
show security key-chain	This command displays the configured keychains in the system.

MIB Objects

```
alaSecKeyChainMappingKeyChainId
alaSecKeyChainMappingKeyId
alaSecKeyChainMappingRowStatus
```

show security key

This command displays the configured keys in the system.

show security key [*key_id* [*-key_id2*]**]**

Syntax Definitions

key_id	The key ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, 9900

Usage Guidelines

If key ID is not provided, information of all the keys is displayed.

Examples

```
-> show security key
ID    Status    Algorithm       Start-time           Life-time
                              (mm/dd/yyyy hh:mm)     (day hh:mm)
----+--------+------------+----------------------+--------------
1     expired   sha256       01/31/2016 10:30        100 00:00
2     valid     sha256       01/31/2016              1000 00:15
10    future    sha256       01/31/2017              180 (default)
24    valid     sha256       01/31/2016 05:00        0    12:20
```

output definitions

ID	The key ID.
Status	The status of the key.
Start-time	Key activation time.
Life-time	Validity duration of the key in terms of days and time.

Release History

Release 8.4.1; command introduced.

Related Commands

security key	This command creates an authentication key into the system.

MIB Objects

```
alasecKeychainId
alasecKeyId
```

show security key-chain

This command displays the configured keychains in the system.

show security key-chain [*key_chain_id***]**

Syntax Definitions

key_chain_id	The keychain ID.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6860, 6865, 6900, 9900

Usage Guidelines

If keychain ID is not provided, information of all the keychains is displayed.

Examples

```
-> show security key-chain
ID        Name             current      Associated           User
                            key          keys              applications
----+------------------+--------+------------------+-------------------------
1     globalKeychain         5          1,3,5-8,10      isis,isis_abc,ospf
2     vlan10Keychain         22         20,22           isis_123
```

output definitions

ID	The keychain ID.
Name	The keychain name.
Current Key	The current active key.
Associated Keys	The keys associated with the keychain.
User Applications	The keychain associated with the user application.

Release History

Release 8.4.1; command introduced.

Related Commands

security key-chain	This command creates a system level security keychain.
security key-chain key	This command associates a key into the specified keychain.

MIB Objects

```
alaSecKeyChainId
alasecKeychainName
```

alarm in

Configures an alarm input. For an alarm input, action can be configured to either send an SNMP trap, log a SWLog message locally, or set alarm output.

alarm in *alr_in_name* **[chassis-in** *chassis_id_in***] action {swlog | trap | alarm-out} [admin-state {enable | disable}]**

no alarm *alr_in_name*

Syntax Definitions

alr_in_name	Name of the alarm input (1 to 32 characters).
chassis_id_in	Chassis identifier where alarm input is connected.
swlog | trap | alarm-out	Specify the action to be sent on the alarm output.
enable	Enable the alarm input.
disable	Disable the alarm input.

Defaults

parameter	default
enabled | disabled	disable

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- By default, alarm is disabled for all actions.
- If the chassis ID is not configured, by default, local chassis is considered for the alarm input.
- Use the **no** form of this command to remove the alarm input.
- OmniSwitch 6465 switch has a single alarm input.

Examples

```
-> alarm in "temperature-sensor" action alarm-out
-> alarm in "door-sensor" chassis-in 1 action alarm-out admin-state enable
-> alarm in "smoke-sensor" chassis-in 2 action trap swlog alarm-out admin-state
enable

-> no alarm temperature-sensor
```

Release History

Release 8.5 R1; command introduced.

Related Commands

alarm clear status	Clears the status of the specified alarm.
show alarm input config	Displays the alarm input configuration.
show alarm status	Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

```
alaAlarmInpmutConfigTable
   alaAlarmInputConfigName
   alaAlarmInputConfigChassis
   alaAlarmConfigInputTrapActionEnable
   alaAlarmConfigInputSwlogActionEnable
   alaAlarmConfigInputAlarmOutputActionEnable
   alaAlarmConfigAdminStatus
   alaAlarmInputConfigRowStatus
```

alarm event

Configures the listed system events or any trap for alarm output.

alarm event *alr_event_name* **{event {vc-status-change | temperature | system-health | power-supply | port-violation network-port** *userport* **[-***userport2*] **| port-health | link-down network-port** *userport* **[-***userport2*] **| authentication-failure} | trapid** *id***}} [chassis-in** *chassis_id_in***] [admin-state {enable | disable}]**

no alarm *alr_event_name*

Syntax Definitions

alr_event_name	Name of the alarm event or trap (1 to 32 characters).
userport	Network port of the switch.
id	Trap ID.
chassis_id_in	Chassis identifier where alarm input is connected.
enable	Enable the alarm event.
disable	Disable the alarm event.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- By default, alarm output action is disabled for all the alarm events.
- System events corresponds to critical failures of the switch. Alarm event can be configured for any of these supported system events.
- Trap ID corresponds to the SNMP traps supported in the switch. Use **show snmp-trap config** command to view the supported traps. Alarm event can be configured for any of these supported traps.
- Both event as well as trap cannot be configured for the same alarm event. If configured, the later is ignored with an error message.
- Alarm event of the single chassis can be mapped to multiple alarm outputs on different chassis for redundancy.
- Alarm events from multiple chassis can be mapped to alarm output on the single chassis.
- Same network port can be configured for both link down as well as port violation event but with a different event name.

- A network port that falls in the network port range, which is already configured to an event cannot be configured to another event.
- If the chassis ID is not configured, by default, local chassis is considered for the alarm event.
- Use the **no** form of this command to remove the alarm event.

Examples

```
-> alarm event system-fail event system-health
-> alarm event link-failure-critical event link-Down network-port 10-15 chassis-in
1 admin-state enable

-> no alarm system-fail
```

Release History

Release 8.5 R1; command introduced.

Related Commands

alarm clear status	Clears the status of the specified alarm.
show alarm event config	Displays the alarm system event configuration.
show alarm status	Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

```
alarmEventConfigTable
   alarmEventConfigTable
   alarmEventConfigName
   alarmEventConfigEvent
   alarmEventConfigTrapId
   alarmEventConfigNetworkPortStart
   alarmEventConfigNetworkPortEnd
   alarmEventConfigInputChassis
   alarmEventConfigAdminStatus
   alaAlarmEventConfigRowStatus
```

alarm out

Configures the alarm output relay of a chassis.

alarm out *alr_out_name* **[chassis-out** *chassis_id_out***] [admin-state {enable | disable}]**

no alarm out *alr_out_name*

Syntax Definitions

alr_out_name	Name of the alarm output (1 to 32 characters).
chassis_id_out	Chassis identifier where alarm output is connected.
enable	Enable the alarm output.
disable	Disable the alarm output.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- If the chassis ID is not configured, by default, local chassis is considered for the alarm output.
- Use the **no** form of this command to remove the alarm output.
- OmniSwitch 6465 switch has single alarm output.

Examples

```
-> alarm out "critical-fault-detector"
-> alarm out "minor-fault-detector" chassis-out 2 action admin-state enable
-> alarm out "critical-fault-detector"
```

Release History

Release 8.5 R1; command introduced.

Related Commands

show alarm status	Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

```
alaAlarmOutputConfigTable
   alaAlarmOutputConfigName
   alaAlarmOutputConfigChassis
   alaAlarmOutputConfigRowStatus
```

alarm map

Maps an alarm input or event with an alarm output within a chassis or any other chassis in the VC.

alarm map *alarm_name* **out** *alr_out_name*

no alarm map *alarm_name*

Syntax Definitions

alarm_name	Name of the alarm input or system event (1 to 32 characters).
alr_out_name	Name of the alarm output (1 to 32 characters)

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Alarm input or event of the single chassis can be mapped to multiple alarm outputs on different chassis for redundancy.
- Alarm input or event from multiple chassis can be mapped to alarm output on the single chassis.
- Use the **no** form to unmap the alarm input from alarm output.

Examples

```
-> alarm map "temperature-sensor" out "critical-fault-detector"
-> no alarm map "temperature-sensor"
```

Release History

Release 8.5 R1; command introduced.

Related Commands

alarm in	Configures an alarm input.
alarm event	Configures the listed system events or any trap for alarm output.
alarm out	Configures the alarm output relay of a chassis.
show alarm status	Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

```
alaAlarmMappingConfigTable
   alaAlarmInputConfigName
   alaAlarmOutputConfigName
   alaAlarmMappingConfigRowStatus
```

alarm duration

Configure the duration of an alarm.

alarm duration [[*hour*] **[***min*] | **[default]]**

Syntax Definitions

hour	Duration of the alarm in hours.
min	Duration of the alarm in minutes.
default	Sets the alarm duration to 24 hours 0 minutes.

Defaults

By default, the alarm duration is set to 24 hours 0 minutes.

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- In a virtual chassis (VC) setup, alarm duration configuration applies to all the chassis of the VC.
- A minimum alarm duration of five minutes and a maximum alarm duration of 48 hours can be configured.
- An alarm is switched off for an input or event after the configured duration. If there are multiple events or input, alarm is switched off after the elapsed duration of all the events and input.
- Use **alarm clear status** command to force stop the alarm before the set alarm duration for any alarm event or input.
- Modification or updated duration is applied only to those alarms raised after the configuration change. Alarms which are in progress are not impacted.
- Use **default** option to reset the alarm duration to 24 hours 0 minutes.

Examples

```
-> alarm duration 2
-> alarm duration default
```

Release History

Release 8.5 R1; command introduced.

Related Commands

alarm clear status	Clears the status of the specified alarm.
show alarm status	Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

```
alarmDurationConfigHour
alarmDurationConfigMin
```

alarm clear status

Clears the status of the specified alarm.

alarm clear status [*alarm_name***]**

Syntax Definitions

alarm_name	Name of the alarm input or alarm event.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- The command does not disable or remove the alarm.
- The command can be used to forcibly stop the alarm and clear the status.
- If the output alarm is ON for multiple events or input, all the alarms have to be cleared to switch off the alarm output.
- If the alarm name is not specified, all the configured alarms are cleared.

Examples

```
-> alarm clear status temperature-sensor
-> alarm clear status
```

Release History

Release 8.5 R1; command introduced.

Related Commands

show alarm status	Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

```
alarmStatusTable
   alarmStatusInputName
   alarmStatusOutputName
   alarmStatusInputChassis
   alarmStatusOutputChassis
   alarmStatusTimeStamp
   alarmStatusTrapid
```

show alarm input config

Displays the alarm input configuration.

show alarm input config chassis *chassis_id*

Syntax Definitions

chassis_id	Chassis identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

The command displays configuration of all the chassis if chassis ID is not specified.

Examples

```
-> show alarm input config
Alarm Duration 5 hrs 30 Mins

Alarm-Name         Chassis-in    Action       Alarm-Output-Name      Chassis-out    Admin-State
-----------------+----------+-------------+----------------------+--------------+-------------
Temperature Sensor     1       Alarm-Output  critical-fault-detector      1           enable
fire Sensor            1       trap              N/A                      N/A         enable
Temperature Sensor     1       Alarm-Output   minor-fault-detector        2           enable
door Sensor            1       Alarm-Output   minor-fault-detector        2           enable
```

output definitions

Alarm-Name	Name of the alarm.
Chassis-in	Chassis identifier where alarm input is connected.
Action	The action sent on the alarm output.
Alarm-Output-Name	Name of the alarm output.
Chassis-out	Chassis identifier where alarm output is connected.
Admin-State	Status of the alarm.

Release History

Release 8.5 R1; command introduced.

Related Commands

alarm in	Configures an alarm input.
show alarm status	Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

```
alaAlarmInputConfigTable
   alaAlarmInputConfigName
   alaAlarmInputConfigChassis
   alaAlarmConfigInputTrapActionEnable
   alaAlarmConfigInputSwlogActionEnable
   alaAlarmConfigInputAlarmOutputActionEnable
   alaAlarmConfigAdminStatus
   alaAlarmInputConfigRowStatus
alaAlarmInputConfigTable
   alaAlarmOutputConfigName
   alaAlarmOutputConfigChassis
   alaAlarmOutputConfigRowStatus
alaAlarmMappingConfigTable
   alaAlarmInputConfigName
   alaAlarmOutputConfigName
   alaAlarmMappingConfigRowStatus
```

show alarm event config

Displays the alarm system event configuration.

show alarm event config chassis *chassis-id*

Syntax Definitions

chassis_id	Chassis identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- The command displays configuration of all the chassis if chassis ID is not specified.
- Network port is only applicable for link-down and port violation event.

Examples

```
-> show alarm event config
Alarm Duration 5 hrs 30 Mins

Alarm-Name     Chassis-In   Network-Port Trap-Id   Event-Name    Alarm-Output-Name    Chassis_out  Admin-State
-------------+------------+-------------+-------+-------------+--------------------+------------+------------
system-fail       1            N/A        N/A    system-health  minor-fault-detector      2          enable
power-fail        1            N/A        N/A    power-supply   minor-fault-detector      2          enable
login-failure     2            N/A         5      N/A           minor-fault-detector      2          enable
```

output definitions

Alarm-Name	Name of the alarm.
Chassis-in	Chassis identifier where alarm input is connected.
Network-Port	Network port of the chassis.
Trap-ID	Trap ID.
Event-Name	Name of the system event.
Alarm-Output-Name	Name of the alarm output.
Chassis-out	Chassis identifier where alarm output is connected.
Admin-State	Status of the alarm.

Release History

Release 8.5 R1; command introduced.

Related Commands

alarm event	Configures the listed system events or any trap for alarm output.
show alarm status	Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

```
alarmEventConfigTable
   alarmEventConfigName
   alarmEventConfigEvent
   alarmEventConfigTrapId
   alarmEventConfigNetworkPortStart
   alarmEventConfigNetworkPortEnd
   alarmEventConfigInputChassis
   alarmEventConfigAdminStatus
   alaAlarmEventConfigRowStatus
alaAlarmOutputConfigTable
   alaAlarmOutputConfigName
   alaAlarmOutputConfigChassis
   alaAlarmOutputConfigRowStatus
alaAlarmMappingConfigTable
   alaAlarmInputConfigName
   alaAlarmOutputConfigName
   alaAlarmMappingConfigRowStatus
```

show alarm status

Displays all the traps, system events, or alarm input for which the alarm output is raised. For a VC, the alarm status for each chassis is displayed.

show alarm status chassis *chassis-id*

Syntax Definitions

chassis_id	Chassis identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6465

Usage Guidelines

- Network port displays the status on the port range or a specific port.
- If the same failure (input or event or trap) is repeated, the data structure is updated with the latest failure.

Examples

```
-> show alarm status chassis-id 2

Alarm-Name    Chassis-In     Time-Stamp         Network-Port  Trap-Id Event-Name   Alarm-Output     Chassis-Out
------------+----------+---------------------+------------+--------+----------+-----------------+-----------
login-failure    2        09/31/2017 : 14:30:00      N/A        5       N/A      minor-fault-detector   2
```

output definitions

Alarm-Name	Name of the alarm.
Chassis-in	Chassis identifier where alarm input is connected.
Time-Stamp	The system time of the switch where the alarm occurred.
Network-Port	Network port of the chassis.
Trap-ID	Trap ID.
Event-Name	Name of the system event.
Alarm-Output	Name of the alarm output.
Chassis-out	Chassis identifier where alarm output is connected.

Release History

Release 8.5 R1; command introduced.

Related Commands

show alarm input config	Displays the alarm input configuration.
show alarm event config	Displays the alarm system event configuration.

MIB Objects

```
alarmStatusTable
   alarmStatusInputName
   alarmStatusOutputName
   alarmStatusInputChassis
   alarmStatusOutputChassis
   alarmStatusTimeStamp
   alarmStatusTrapid
   alarmStatusEvent
   alarmStatusNetworkPortStart
   alarmStatusNetworkPortEnd
   alarmStatusClear
```

appmgr

Use this command to start the tasks for AOS Micro Services (AMS).

appmgr {start | stop | restart} [ams *broker* **| config-sync | config-dbase] [ams-apps iot-profiler**]

Syntax Definitions

start	Starts the specified application from package.
stop	Stops the specified application from package.
restart	Starts and stops the specified application from package.
broker	Broker instance of AMS
config-sync	An AMS component application which is used to synchronize the configuration in the network.
config-dbase	Another AMS component application that helps to store and replay the configuration to new nodes in the network.
iot-profiler	An AMS-app application, responsible for sharing the IoT profiled data with OmniVista for the integrated IoT OV-Switch solution.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

Enter **appmgr** without any parameters to see the command syntax.

Examples

```
-> appmgr start ams broker
-> appmgr start ams config-sync
-> appmgr start ams config-dbase
-> appmgr commit
-> appmgr list
Legend: (+) indicates application is not saved across reboot

  Application    Status    Package Name        User/Group            Status Time Stamp
---------------+---------+------------------+--------------------+--------------------
broker           started   ams              admin/user          Tue Nov 26 13:28:27 2019
config-sync      started   ams              admin/user          Tue Nov 26 13:28:27 2019
config-dbase     started   ams              admin/user          Tue Nov 26 13:28:27 2019
iot-profiler     started   ams              admin/user          Tue Nov 26 13:28:27 2019

-> appmgr start ams-apps iot-profiler -args -h 10.10.10.1 -p 1883
Success to start iot-profiler
```

Release History

Release 8.6R1; command introduced.
Release 8.6R2; command syntax and command output modified.

Related Commands

appmgr list	Displays the application currently launched/stopped/committed.
appmgr commit	Use this command to save the configuration across reboots.

MIB Objects

N/A

appmgr list

Displays the application currently started/stopped/committed.

appmgr list [*app_name***]**

Syntax Definitions

app_name	Specify the name of the application.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

Enter **appmgr** without any parameters to see the command syntax.

Examples

```
-> appmgr list
Legend: (+) indicates application is not saved across reboot
 Application      Status    Package Name   User/Group     Status TimeStamp
---------------+---------+------------------+--------------------+-------------
+ broker          stopped      ams       admin/user    Mon Nov 25 17:07:54 2019
  config-sync     started      ams       admin/user    Tue Nov 12 11:43:12 2019
  config-dbase    started      ams       admin/user    Tue Nov 12 11:43:39 2019

-> appmgr list iot-profiler
Package Name            : ams-apps
Committed (Yes/No)      : No
Status                  : started
Timestamp               : Apr 16, 2014: 02:20:02
User/Group              : admin/user
Command line arguments  : -h 10.10.10.1 -p 1883
Installation script     : /flash/working/pkg/ams-apps/install.sh
```

output definitions

Application	Displays the name of the Application.
Status	Displays the status of the Application.
Package Name	Displays the name of the package.
User/Group	Displays the user/group information.
Status TimeStamp	Displays the timestamp status information.

Release History

Release 8.6R2; command introduced.

Related Commands

appmgr	Use this command to start the tasks for AOS Micro Services (AMS).
appmgr commit	Use this command to save the configuration across reboots.

MIB Objects

N/A

appmgr commit

Use this command to save the configuration across reboots.

appmgr commit

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

Enter **appmgr** without any parameters to see the command syntax.

Examples

```
-> appmgr commit
```

Release History

Release 8.6R2; command introduced.

Related Commands

appmgr	Use this command to start the tasks for AOS Micro Services (AMS).
appmgr list	Displays the application currently started/stopped/committed.

MIB Objects

N/A

pkgmgr

Use this command to install Debian packages for non-AOS software applications (like AMS and WebView 2.0).

pkgmgr {[install | verify] *package_file_name* **| remove** *package_name***}**

Syntax Definitions

install	Extracts and installs the contents of the package to system memory.
remove	Removes all the files of this package from system memory.
verify	Verifies the ALE signature and the checksums for the Debian package.
package_file_name	Name of the Debian package file
package_name	Name of the package displayed in output of **pkgmgr list** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

- Enter **pkgmgr** without any parameters to see the command syntax.
- The Debian package must be downloaded from the service and support website (businessportal2.alcatel-lucent.com).
- The Debian package file must be copied to the *pkg* in the running directory. For example, if working is the running directory, then copy to */flash/working/pkg* directory of the switch.
- Use the **pkgmgr verify** command to verify the contents of the package.
- Use the **pkgmgr install** command to install the package.
- After the package is installed successfully, use the **pkgmgr commit** command to save the installation permanently.
- If the switch restricts installation of the package due to memory threshold, use the **health threshold memory** command to increase the RAM memory of the switch.
- Use the **pkgmgr remove** command to remove the package.

Note. In a Virtual Chassis environement, if this **pkgmgr** command is successful on Master unit, it will be automatically executed on all units of the Virtual Chassis.

Examples

```
-> pkgmgr verify ams-8.6.R02-6235.deb
CLI output:
Verifying MD5 checksum.. OK

-> pkgmgr install ams-8.6.R02-6235.deb

Verifying MD5 checksum.. OK
System Memory check.. PASS
Preparing to replace ams-8.6.R02-6235 (using /flash/working/pkg/ams-8.6.R02-
6235.deb)...
Setting up ams (8.6.R02-6235.deb)...
Extracting control files for package ams-8.6.R02-6235.deb .. OK
Installing package ams-8.6.R02-6235.deb .. OK

-> pkgmgr commit

-> pkgmgr remove ams
CLI output:
Purging ams (8.6.R02-6235)...
Removing package ams.. OK

-> pkgmgr verify package-webview-8.6.R02-168.deb
CLI output:
Verifying MD5 checksum.. OK

-> pkgmgr install package-webview-8.6.R02-168.deb
Verifying MD5 checksum.. OK
System Memory check.. PASS
Preparing to replace package-webview-8.6.R02-168.deb (using /flash/working/pkg/
package-webview-8.6.R02-168.deb)...
Setting up webview (package-webview-8.6.R02-168.deb)...
Extracting control files for package package-webview-8.6.R02-168.deb .. OK
Installing package package-webview-8.6.R02-168.deb .. OK

-> pkgmgr commit

-> pkgmgr remove webview
CLI output:
Purging webview (package-webview-8.6.R02-168.deb)...
Removing package webview.. OK
```

Release History

Release 8.6R2; command introduced.

Related Commands

pkgmgr list	Displays the packages currently installed/committed.
pkgmgr commit	Use this command to save all ‘installed’ packages so that they can be restored after reboot.

MIB Objects

N/A

pkgmgr list

Displays the packages currently installed/committed.

pkgmgr list [*package_name***]**

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

Enter **pkgmgr** without any parameters to see the command syntax.

Examples

```
-> pkgmgr list ams
Package Name            : ams,
Committed (Yes/No)      : Yes,
Version                 : default,
Filename                : ams-8.6.R02-6235,
Status                  : installed,
Timestamp               :  ,
User/Group              : root/root,
Installation script     : default
```

output definitions

Package Name	Displays the name of the package.
Committed (Yes/No)	Displays whether the package is committed or not.
Version	Displays the version of the package.
Filename	Displays the filename.
Status	Displays the status of the package.
Timestamp	Displays the timestamp.
User/Group	Displays the name of user and group.
Install Script	Displays the install script details.

Release History

Release 8.6R2; command introduced.

Related Commands

pkgmgr	Use this command to install the required non-AOS software applications (developed by ALE and/or ALE-approved partners) Debian package.
pkgmgr commit	Use this command to save all ‘installed’ packages so that they can be restored after reboot.

MIB Objects

N/A

pkgmgr commit

Use this command to save all ‘installed’ packages so that they can be restored after reboot.

pkgmgr commit

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900, OmniSwitch 6900-V72, 6900-C32

Usage Guidelines

Enter **pkgmgr** without any parameters to see the command syntax.

Examples

```
-> pkgmgr commit
```

Release History

Release 8.6R2; command introduced.

Related Commands

pkgmgr	Use this command to install the required non-AOS software applications (developed by ALE and/or ALE-approved partners) Debian package.
pkgmgr list	Displays the packages currently installed/committed.

MIB Objects

N/A

59 Chassis MAC Server (CMS) Commands

The Chassis MAC Server (CMS) manages MAC addresses on the switch. The MAC addresses managed via the CMS are used as identifiers for the following functions:

- Base chassis MAC address
- Ethernet Management Port (EMP)
- VLAN router ports

Similar to IP addresses, MAC addresses are assigned by the Internet Assigned Numbers Authority (IANA) and distributed to users in sequential blocks. A sequential block of MAC addresses is referred to as a MAC address *range*.

The MAC address range is stored on the switch's EEPROM. The switch supports one MAC address range only. By default, this MAC address range contains thirty-two (32) factory-installed, contiguous MAC addresses.

MIB information for the Chassis MAC Server commands is as follows:

Filename: ALCATEL-IND1-MAC-SERVER-MIB.mib
Module: alcatelIND1MacServerMIB

A summary of the available commands is listed here:

mac-range eeprom
show mac-range
show mac-range alloc

mac-range eeprom

Modifies the default MAC range on the switch's EEPROM.

Note. Use caution when modifying the default MAC range. Improper use of this command can disable your system and adversely affect your network. Contact Alcatel-Lucent Enterprise Customer Support for further assistance.

mac-range eeprom *start_mac_address count*

Syntax Definitions

start_mac_address	The first MAC address in the modified range. Enter the MAC address in the following format: **xx:xx:xx:xx:xx:xx**, where **x** is a hex value (0–f).
count	Specifies the number of MAC addresses in the range (1–256).

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Because the factory-installed 32 MAC addresses are sufficient for most network configurations, this command should only be used by qualified network administrators for special network requirements.
- After modifying a MAC address range by using the **mac-range eeprom** command, you must reboot the switch. Otherwise, MAC addresses for existing VLAN router ports will not be allocated properly.
- All MAC addresses in a range must be contiguous (i.e., there cannot be any gaps in the sequence of MAC addresses).

Examples

```
-> mac-range eeprom 00:20:da:23:45:35 32
```

Release History

Release 7.1.1; command introduced.

Related Commands

show mac-range	Displays the MAC range table.

MIB Objects

```
chasMacAddressRangeTable
   chasMacRangeIndex
   chasGlobalLocal
   chasMacAddressStart
   chasMacAddressCount
```

show mac-range

Displays the MAC range table.

show mac-range [*index***]**

Syntax Definitions

index	Identifies the MAC range by referring to its position in the MAC range table.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Because the switch currently supports one MAC address range only, index position 1 displays.

Examples

```
-> show mac range

 Mac                    Local/
Range  Row Status       Global   Start Mac Addr     End Mac Addr
-----+----------------+--------+-----------------+-----------------

01     ACTIVE           GLOBAL   00:d0:95:6a:79:6e  00:d0:95:6a:79:8d
```

output definitions

Mac Range	The MAC range index number (1). Because the switch currently supports one MAC address range only, index position 1 displays.
Row Status	The current status of the MAC range. The status **ACTIVE** refers to MAC addresses that are available for allocation to VLAN router ports and other applications.
Local/Global	The Local/Global status for MAC addresses in the range. Local MAC addresses have the local bit set in the first byte of the address. Global MAC addresses (also referred to as *EEPROM* MAC addresses) have the global bit set in the first byte of the address and are stored on the switch's EEPROM. Because the switch's default MAC range is stored on EEPROM, the status GLOBAL displays.
Start Mac Addr	The first MAC address in the MAC address range.
End Mac Addr	The last MAC address in the MAC address range.

Release History

Release 7.1.1; command introduced.

Related Commands

mac-range eeprom	Modifies the default MAC range on the switch's EEPROM.

MIB Objects

```
chasMacAddressRangeTable
   chasMacRangeIndex
   chasGlobalLocal
   chasMacAddressStart
   chasMacAddressCount
   chasMacRowStatus
```

show mac-range alloc

Displays all allocated addresses from the MAC range table.

show mac-range [*index***] alloc**

Syntax Definitions

index	Identifies the MAC range by referring to its position in the MAC range table. Currently, index position 1 only is supported.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show mac-range alloc
Range    Mac Address         Application     Id
-----+-----------------+--------------------+---
01    00:d0:95:6b:09:40 CHASSIS              0
01    00:d0:95:6b:09:41 802.1X               0
01    00:d0:95:6b:09:5f CHASSIS              1
```

output definitions

Range	The MAC range's index number. The index number refers to the position of the range in the MAC range table. Values may range from 1–20. MAC ranges are divided by index number into four distinct categories. Refer to page 59-4 for more information.
Mac Address	Current MAC address allocated for a specific application.
Application	The application for which the allocated MAC address is being used. Current options include **VLAN, 802.1X**, and **CHASSIS**. VLAN refers to MAC addresses allocated to VLAN router ports in multiple MAC router mode. CHASSIS refers to MAC addresses used for the base chassis MAC address and the Ethernet Management Port (EMP).

output definitions (continued)

Id	An ID number used to identify an allocated MAC address. ID numbers are used for the base chassis MAC address and Ethernet Management Port (EMP), as well as VLAN router ports. The ID value 0 is reserved for the switch's base chassis MAC address. The ID value 1 is reserved for the EMP MAC address. Router ports assigned to VLANs 2 through 4094 are given corresponding MAC IDs. For example, a router port configured on VLAN 44 receives an allocated MAC ID of 44. Because default VLAN 1 router ports use the base chassis MAC address by default, any router port configured on VLAN 1 is assigned the ID value 0.

Release History

Release 7.1.1; command introduced.

Related Commands

mac-range eeprom	Modifies the default MAC range on the switch’s EEPROM.

MIB Objects

```
ChasMacAddressAllocTable
   chasAppId
   chasObjectId
   chasAllocMacRangeIndex
   chasAllocMacAddress
```

60 Network Time Protocol Commands

The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver. It provides client time accuracies within a millisecond on LANs, and up to a few tens of millisecond on WANs. Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability.

It is important for networks to maintain accurate time synchronization between network nodes. The standard timescale used by most nations of the world is based on a combination of Universal Coordinated Time (UTC) (representing the Earth's rotation about its axis) and the Gregorian Calendar (representing the Earth's rotation about the Sun). UTC time is disseminated by various means, including radio and satellite navigation systems, telephone modems, and portable clocks.

The MIB information for NTP is as follows:

Filename: ALCATEL-IND1-NTP-MIB.mib
Module: alcatelIND1NTPMIB

A summary of available commands is listed here:

ntp server
ntp server synchronized
ntp server unsynchronized
ntp client
ntp src-ip preferred
ntp broadcast
ntp broadcast-client
ntp broadcast-delay
ntp key
ntp key load
ntp authenticate
ntp master
ntp interface
ntp max-associations
ntp broadcast
ntp peer
ntp vrf-name
show ntp status
show ntp client
show ntp client server-list
show ntp server client-list
show ntp server status
show ntp keys
show ntp peers
show ntp server disabled-interfaces

ntp server

Specifies an NTP server from which the switch will receive updates.

ntp server {*ip_address* | *server_name*} **[key** *key_id* **| | minpoll** *poll* | **maxpoll** *poll* | **version** *version* | **prefer | burst | iburst | preempt]**

no ntp server *ip_address*

Syntax Definitions

ip_address	The IP address of the NTP server to be added or deleted to the client's server list.
server_name	Fully qualified NTP server domain name.
key_id	The key identification number that corresponds to the specified NTP server. The value ranges from 0 to 65534. 0 can be used to unconfigure the key ID.
minpoll *poll*	It specifies the minimum polling interval for NTP messages, in seconds. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds ($2^4 = 16$). The minimum poll interval defaults to 6 (64 s), but can be decreased by the minpoll option to a lower limit of 3 (8 s) and an upper limit of 17 (36.4h).
maxpoll *poll*	It specifies the maximum polling interval for NTP messages, in seconds. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the maximum poll time would be 16 seconds ($2^4 = 16$). The maximum poll interval defaults to 10 (1,024 s), but can be increased by the maxpoll option to an upper limit of 17 (36.4 h) and a lower limit of 3 (8 s). The maxpoll must not be less than the minpoll value.
version	The version of NTP being used. This will be 1, 2, 3, or 4.
prefer	Marks this server as the preferred server. A preferred server's timestamp will be used before another server.
burst	Enables burst mode. The burst mode allows the exchange of eight NTP messages (instead of one) when the server is reachable and at each poll interval to achieve faster synchronization. The spacing between the first and the second packet is 16 seconds to allow a modem call to complete, while the spacing between the remaining packets is 2 seconds.
iburst	Enables initial burst (iburst) mode. The iburst mode allows immediate exchange of eight NTP messages (instead of one) when the server is unreachable and at each poll interval, to achieve faster initial synchronization acquisition. The spacing between the packets is 16 seconds to allow a modem call to complete. Once the server is reachable, the spacing between the packets is 2 seconds.
preempt	Enables the preemption mode for the server rather than the default persistent.

Defaults

Parameter	Default
version	4
minpoll *poll*	6
maxpoll *poll*	10
prefer	not preferred
burst	no burst
iburst	no iburst

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to clear an NTP server from the list of configured servers.
- To configure NTP in the client mode you must first define the NTP servers. Up to 12 NTP servers may be defined.
- Either an IP address or domain name for the specified server can be entered.
- The NTP key identification is an integer. It corresponds to an MD5 authentication key contained in an authentication file (.txt) located on the server. This file must be on both the server and the local switch, and match, for authentication to work. Enter the key identification using the **key** keyword if the server is set to MD5 authentication.
- An authentication key is composed of a 32-bit integer and 32-byte string of characters. The integer format is hexadecimal. For an NTP message to be authenticated the NTP client authentication key must match the key configured at the NTP server. This means the authentication keys must be distributed in advance of configuring the NTP client. If authentication is disabled but authentication key is present, the association will still be unauthenticated.
- Use the **version** keyword to set the correct version of NTP.
- Use the **minpoll** keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds ($2^4 = 16$). The client will poll the server for a time update when the **minpoll** time is exceeded.
- Use the **maxpoll** keyword to specifies the maximum polling interval for NTP messages. This number is determined by raising 2 to the power of the number entered. The maximum poll interval defaults to 10 (1,024 s), but can be increased by the maxpoll option to an upper limit of 17 (36.4 h) and a lower limit of 3 (8 s). The maxpoll must not be less than the minpoll value.
- NTP authentication must be disabled before adding or removing an NTP server.
- Burst mode of operation improves timekeeping quality with the server command and iburst mode of operation is designed to speed the initial synchronization acquisition with the server command.
- When preempt is enabled, the specified server is marked unavailable for selection if any error (authentication failure) is detected on a connection between the local device and reference clock. The

server is marked available for selection if no other connections are available and no error is detected on the connection between the local device and reference clock.

Examples

```
-> ntp server 1.1.1.1
-> ntp server 0.pool.ntp.org
-> ntp server 1.1.1.1 key 1
-> ntp server 1.1.1.1 version 4
-> ntp server 0.pool.ntp.org minpoll 5
-> ntp server 0.pool.ntp.org maxpoll 6
-> ntp server 1.1.1.1 burst
-> ntp server 1.1.1.1 iburst
-> ntp server 1.1.1.1 prempt
-> no ntp server 1.1.1.1
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R4: **server name**, **maxpoll, burst**, **iburst, prempt** keywords added.

Related Commands

ntp client	Enables or disables NTP operation on the switch.
show ntp client server-list	Displays a list of the servers with which the NTP client synchronizes.
show ntp server status	Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

```
alaNtpConfig
   aalaNtpPeerIpAddress
   alaNtpPeerType
   alaNtpPeerAuth
   alaNtpPeerVersion
   alaNtpPeerMinpoll
   alaNtpPeerPrefer
   alaNtpPeerAdminalaNtpPeerName
   alaNtpPeerBurst
   alaNtpPeerIBurst
   alaNtpPeerPreempt
   alaNtpPeerMaxpoll
```

ntp server synchronized

Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.

ntp server synchronized

Syntax Definitions

N/A

Defaults

By default, NTP synchronization is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The NTP protocol discards the NTP servers that are unsynchronized. However, the unsynchronized NTP servers are used as network time sources.

Examples

```
-> ntp server synchronized
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; command deprecated.

Related Commands

ntp server unsynchronized	Disables an NTP client from invoking tests for NTP server synchronization. This allows the NTP client to synchronize with unsynchronized NTP servers in the network.

MIB Objects

```
alaNtpConfig
   alaNtpPeerTests
```

ntp server unsynchronized

Disables an NTP client from invoking tests for NTP server synchronization. This allows the NTP client to synchronize with unsynchronized NTP servers in the network.

ntp server unsynchronized

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When NTP peer synchronization tests are disabled, the NTP client is able to synchronize with either an NTP peer that is not synchronized with an atomic clock or a network of NTP servers that will finally synchronize with an atomic clock.

Examples

```
-> ntp server unsynchronized
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; command deprecated.

Related Commands

ntp server synchronized	Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.

MIB Objects

```
alaNtpConfig
   alaNtpPeerTests
```

ntp client

Enables or disables NTP time synchronization discipline.

ntp client admin-state {enable | disable}

Syntax Definitions

enable	Enables NTP.
disable	Disables NTP.

Defaults

NTP protocol is disabled by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to enable or disable NTP. Before NTP can be enabled, an NTP server must be specified using the **ntp server** command. Up to 12 NTP servers may be defined.
- It is not necessary to specify an NTP server if the NTP client will only receive time updates from NTP broadcast servers.
- NTP client will not synchronize with an unsynchronized NTP server (Stratum 16).

Examples

```
-> ntp client enable
-> ntp client disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ntp server	Specifies an NTP server from which the switch will receive updates.

MIB Objects

```
alaNtpEnable
```

ntp src-ip preferred

Configures a source IP address to use as the source for NTP packets.

ntp src-ip preferred {default | no-loopback0 | *ip_address***}**

no ntp src-ip preferred

Syntax Definitions

default	The Loopback0 address, if configured, will be used for the source IP address field. If no Loopback0 is configured, the EMP-VC IP address will be used. If no EMP-VC IP address is configured, the preferred IP address will be used. If no preferred IP address is configured the first available IP address on the switch will be used.
no-loopback0	The Loopback0 address will not be used for the source IP address field and either the preferred IP address (if configured) or the first available IP address on the switch will be used.
ip_address	The IP address to be used in the source IP field.

Defaults

By default, the NTP source IP preferred setting is set to the **default** parameter.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- By default The Loopback0 address, if configured, will be used for the source IP address.
- If no Loopback0 is configured, the VC-EMP IP address will be used for the source IP address.
- If no VC-EMP IP address is configured, the preferred IP address will be used for the source IP address.
- If no preferred IP address is configured the first available IP address on the switch will be used as the source IP address.
- When configuring a preferred IP address, that address must already exist on the switch.
- If the configured preferred IP address is the same as the IP address that would have been automatically chosen by the switch, then the ‘ntp src-ip preferred’ command will not be included in the output of the ‘configuration snapshot’ command since only non-default settings are included in the output.
- Use the **no** form of this command to clear a specific IP address and change the behavior back to default.

Examples

```
-> ntp src-ip preferred 192.168.10.1
-> ntp src-ip preferred no-loopback0
-> ntp src-ip preferred default
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; command deprecated.

Related Commands

show ntp status	Displays the NTP configuration and status.

MIB Objects

N/A

ntp broadcast-client

Enables or disables the NTP client to receive time updates from NTP broadcast servers.

ntp broadcast-client {enable | disable}

Syntax Definitions

enable	Enables the client broadcast mode.
disable	Disables the client broadcast mode.

Defaults

Broadcast mode is disabled by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Broadcast mode is intended for operation on networks with numerous workstations and where the highest accuracy is not required. In a typical scenario, one or more time servers on the network broadcast NTP messages that are received by NTP hosts. Correct time is determined from this NTP message based on a pre-configured latency or broadcast delay in the order of a few milliseconds.
- In order to configure NTP in broadcast client mode, it is required to define the network server to client broadcast delay.

Examples

```
-> ntp broadcast-client enable
-> ntp broadcast-client disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ntp broadcast-delay	Sets the broadcast delay time in microseconds.

MIB Objects

```
alaNtpBroadcastEnable
```

ntp broadcast-delay

Sets the broadcast delay time in microseconds of received NTP broadcast messages.

ntp broadcast-delay *microseconds*

Syntax Definitions

microseconds	The number of microseconds for the broadcast delay.

Defaults

parameter	default
microseconds	4000

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When running in the NTP client broadcast mode, a broadcast delay must be set. The broadcast delay is the number of microseconds added to the timestamp received from a broadcast NTP server.

Examples

```
-> ntp broadcast-delay 1000
-> ntp broadcast-delay 10000
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ntp broadcast	Enables or disables the client's broadcast mode.

MIB Objects

```
alaNtpBroadcastDelay
```

ntp key

Labels the specified authentication key identification as trusted or untrusted.

ntp key *key* **[trusted | untrusted]**

Syntax Definitions

key	The key number matching an NTP server.
trusted	Signifies that the specified key is trusted and can be used for authentication.
untrusted	Signifies that the specified key is not trusted and cannot be used for authentication. Synchronization will not occur with an untrusted authentication key.

Defaults

By default, all authentication key are untrusted.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Authentication keys are stored in a key file and loaded into memory when the switch boots. The keys loaded into memory are not trusted until this command is used.The location of the file containing set of generated authentication keys is /flash/network/ntp.keys.
- Once the keys are loaded into software (on boot up of the switch), they must be activated by being labeled as trusted. A trusted key will authenticate with a server that requires authentication as long as the key matches the server key.
- New keys must be added manually to the key file. A newly added key will not be loaded into the switch software until the **ntp key load** command is issued, or the switch is rebooted.
- An authentication key is composed of a 32-bit integer and 32-byte string of characters. The integer format is hexadecimal. For an NTP message to be authenticated the NTP client authentication key must match the key configured at the NTP server. This means the authentication keys must be distributed in advance of configuring the NTP client. If authentication is disabled but authentication key is present, the association will still be unauthenticated.
- By default all keys read from the ntp.conf key file are untrusted therefore keys must be set to ‘trusted’ status to allow NTP to use the key for authentication.

Examples

```
-> ntp key 5 trusted
-> ntp key 2 untrusted
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ntp key	Sets the public key the switch uses when authenticating with the specified NTP server.
ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpAccessKeyIdTable
   alaNtpAccessKeyIdKeyId
   alaNtpAccessKeyIdTrust
```

ntp key load

Loads the current key file into memory.

ntp key load

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command reloads the key file into the switch memory. This allows for new keys in the key file to be added to the list of keys the switch can use for authentication.
- Newly added keys must be labeled as **trusted** with the **ntp key** command before being used for authentication.
- By default, all authentication keys are untrusted therefore reloading a key file will change any current trusted keys to untrusted status.
- The file ntp.keys is used during the establishment of a set of authentication keys that are used by the NTP protocol. The location of this file is fixed in directory /flash/network.

Examples

```
-> ntp key load
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ntp key	Labels the specified authentication key identification as trusted or untrusted.
ntp server	Specifies an NTP server from which this switch will receive updates.

MIB Objects

```
alaNtpAccessRereadkeyFile
```

ntp authenticate

Enables or disables the authentication on a configured NTP server.

ntp authenticate {enable | disable}

Syntax Definitions

enable	Enables authentication for NTP server.
disable	Disables authentication for NTP server.

Defaults

By default, NTP authentication is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to enable or disable authentication for NTP server.
- Before NTP authentication is enabled, NTP operation should be enabled by using **ntp client** command.
- Before enabling the NTP operation, NTP server must be specified using the **ntp server** command.
- NTP authentication must be disabled before adding or removing an NTP server.

Examples

```
-> ntp authenticate enable
-> ntp authenticate disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ntp status	Displays the information about the current NTP status.

MIB Objects

```
alaNtpAuthenticate
```

ntp master

Specifies the stratum value for unsynchronized switch to act as an authoritative NTP source.

ntp master *stratum_number*

Syntax Definitions

stratum_number	Integer value ranging from 2 to 16.

Defaults

Parameter	Default
stratum_number	16

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to synchronize improved clocks with lower strata value if any of the trustworthy NTP sources comes up.
- Use default value of 16 if switch is not synchronized with itself.
- When the switch is synchronized, the stratum number should correspond to peer/server.

Examples

```
-> ntp master 4
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; command deprecated.

Related Commands

show ntp status	Displays current NTP status.

MIB Objects

```
alaNtpConfig
   alaNtpSysStratum
```

ntp interface

Enables or Disables NTP server functionality for an interface.

ntp interface {*interface_ip***} {enable | disable}**

Syntax Definitions

interface_ip	IP address of an interface on which NTP server functionality is to be disabled.
enable	Enables NTP server functionality on an interface.
disable	Disables NTP sever functionality on an interface.

Defaults

By default, NTP server functionality is enabled on all the interfaces.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to enable or disable the incoming NTP request.
- Disabling the NTP server functionality drops the NTP request on an interface and synchronization information is not sent out.

Examples

```
-> ntp interface 10.10.10.1 disable
-> ntp interface 10.10.10.1 enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ntp status	Displays current NTP status.

MIB Objects

```
alaNtpAccessRestrictedTable
   alaNtpAccessRestrictedIpAddress
```

ntp max-associations

Configures the maximum number of associations on the switch.

ntp max-associations *number*

Syntax Definitions

number	Maximum no of client/server and peer associations. Integer value ranging from 0 to 512.

Defaults

By default, 32 associations are allowed on the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to restrict the number of client/server and peer association.
- The command can be used to change the default value of 32 to any value between 0 to 512.
- The command protects the switch from overwhelming with the NTP requests. When the limit is reached, trap is sent to indicate the switch.

Examples

```
-> ntp max-associations 20
```

Release History

Release 7.1.1; command was introduced.
Release 8.6R2; max value increased to 512.

Related Commands

show ntp status	Displays current NTP status.

MIB Objects

```
alaNtpConfig
   alaNtpMaxAssociation
```

ntp broadcast

Enables NTP to broadcast synchronized information to all the clients in the subnet in the configured interval.

ntp broadcast {*broadcast_addr***} [version** *version***] [minpoll** *poll_interval***]**

no ntp broadcast {*broadcast_addr***}**

Syntax Definitions

broadcast_addr	Subnet for which broadcast updates are regularly sent.
version	NTP version on which the broadcast updates are sent out on the subnet for the clients. Value is 3 or 4.
poll_interval	Polling interval for NTP broadcast message. This value is measured in seconds.

Defaults

Parameter	Default
version	4
poll_interval	6

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to configure NTP to act in broadcast server mode.
- Use the **no** form of this command to remove the configured broadcast servers.This also disables NTP synchronization information being sent for that broadcast subset.
- The NTP broadcast address needs to defined to enable NTP broadcast mode. A maximum of 3 broadcast addresses can be configured.
- Use the **version** keyword to set the correct version of NTP.
- Use the **minpoll** keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered.

Examples

```
-> ntp broadcast 10.145.59.255 version 4 minpoll 5
-> no ntp broadcast 10.145.59.255
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ntp broadcast	Enables or disables the client's broadcast mode.
ntp broadcast-delay	Sets the broadcast delay time in microseconds

MIB Objects

```
alaNtpPeerTable
   alaNtpPeerType
   alaNtpPeerVersion
   alaNtpPeerMinpoll
```

ntp peer

Configures NTP to operate in the symmetric active peering mode.This also enables the establishment of an active symmetric association with the specified remote peer.

ntp peer {*ip_address***} [key** *key_id***] [version** *version***] [minpoll** *poll_interval***]**

no ntp peer {*ip_address***}**

Syntax Definitions

ip_address	IP address of the remote peer.
key_id	Authentication key for the remote peer.
version	NTP packet version to be used for the peer association.
poll_interval	Polling interval for NTP broadcast message. Poll interval which when expires, packets will be sent to the peer.

Defaults

Parameter	Default
version	4
poll_interval	6

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use **no** form of this command to remove the peers that are configured to act in symmetric active mode.This command deletes the symmetric active association with the remote peer.
- Use the **version** keyword to set the correct version of NTP.
- Use the **minpoll** keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered.
- The command should not be used for b(Broadcast), m(Multicast) or r(Reference clock address 127.127.x.x).
- *ip-address* is the mandatory parameter to be entered in the command while key id is the optional parameter. If key id is not specified, then peering will not be authenticated.

Examples

```
-> ntp peer 172.18.16.112
-> no ntp peer 172.18.16.112
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ntp peers	Displays current NTP peer association.

MIB Objects

```
alaNtpPeerTable
   alaNtpPeerType
   alaNtpPeerAuth
   alaNtpPeerVersion
   alaNtpPeerMinpoll
```

ntp vrf-name

Sets the VRF to be used for all NTP operations (both client and server).

ntp vrf-name *name*

Syntax Definitions

name	The name of the VRF to be used for all NTP operations.

Defaults

Parameter	Default
name	default

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ntp vrf-name vrf1
```

Release History

Release 7.3.1; command introduced.

Related Commands

show ntp status	Displays the information about the current NTP status.
show ntp client	Displays information about the current client NTP configuration.

MIB Objects

```
alaIpNtpVrfName
```

show ntp status

Displays the information about the current NTP status.

show ntp status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command displays the information about the status of NTP, which is configured along with other global configuration. See the Examples section for more information.
- If the source IP Configuration is done in default or no-loopback0 then the source ip-address will not be displayed in the output of the **show ntp status** command.

Example

```
-> show ntp status
Current time:                   Mon, Jan 21 2019  7:31:04.685 (UTC),
Last NTP update:                Mon, Jan 21 2019  7:30:10.160 (UTC),
Server reference:               10.10.10.10,
Client mode:                    enabled,
Broadcast client mode:          disabled,
Broadcast delay (microseconds): 4000,
Stratum:                        4,
Maximum Associations Allowed:   32,
Authentication:                 enabled,
VRF Name:                       default
```

Current time	The current time for the NTP client.
Last NTP update	The time of the last synchronization with an NTP server.
Server reference	The source of the time signal, which is the address of the NTP server that provided the currently-used time update.
Client mode	Whether the NTP client software is enabled or disabled.
Broadcast client mode	What NTP mode the client is running in, either client or broadcast.
Broadcast delay	The number of microseconds in the advertised broadcast delay time. This field is absent if the client broadcast mode is disabled.
Stratum	The stratum of the server. The stratum number is the number of hops from a UTC time source.

Max-Association	Maximum association on the switch that restricts the number of client/ server and peer association
Authentication	Whether Authentication is enabled or disabled
VRF Name	Name of the VRF.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; **vrf** parameter added.

Related Command

ntp client	Enables or disables NTP operation on the switch.
ntp server	Specifies an NTP server from which the switch will receive updates
ntp server synchronized	Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.
ntp max-associations	Configures the maximum number of associations on the switch.
ntp master	Specifies the stratum value for unsynchronized switch
ntp broadcast	Enables or disables the client's broadcast mode.
show ntp client	Displays information about the current client NTP configuration.
show ntp client server-list	Displays a list of the servers with which the NTP client synchronizes
show ntp server client-list	Displays the basic server information for a specific NTP server or a list of NTP servers

MIB Objects

```
alaNtpPeerListTable
   alaNtpPeerShowOriginateTime
   alaNtpPeerShowTransmitTime
   alaNtpEnable
   alaNtpBroadcastEnable
   alaNtpBroadcastDelay
   alaNtpPeerTests
   alaNtpPeerStratum
   alaNtpPeerTests
   alaNtpAuthenticate
   alaNtpSrcIpConfig
   alaNtpSrcTp
   alaIpNtpVrfName
```

show ntp client

Displays information about the current client NTP configuration.

show ntp client

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the current configuration parameters for the NTP client. The display is slightly different depending on what has been configured on the client. See the Examples section for more information.

Examples

```
-> show ntp client
Current time:                   Mon, Jan 21 2019  7:31:12.505 (UTC),
Last NTP update:                Mon, Jan 21 2019  7:30:10.160 (UTC),
Server reference:               10.10.10.10,
Client mode:                    enabled,
Broadcast client mode:          disabled,
Broadcast delay (microseconds): 4000,
VRF Name:                       default
```

output definitions

Current time	The current time for the NTP client.
Last NTP update	The time of the last synchronization with an NTP server.
Server reference	The source of the time signal, which is the address of the NTP server that provided the currently-used time update.
Client mode	Whether the NTP client software is enabled or disabled.
Broadcast client mode	What NTP mode the client is running in, either client or broadcast.
Broadcast delay	The number of microseconds in the advertised broadcast delay time. This field is absent if the client broadcast mode is disabled.
VRF Name	Name of the VRF.

Release History

Release 7.1.1; command was introduced.

Related Command

ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpLocalInfo
alaIpNtpVrfName
```

show ntp client server-list

Displays a list of the servers with which the NTP client synchronizes.

show ntp client server-list

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display tabular information on the current NTP client to server association status.

Examples

```
-> show ntp client server-list
Legends: + active peer, - passive peer, = client, * current system peer,
         ^ broadcast server, ' broadcast client
Mode IP Address       Ver   Key   St   when   poll   reach   Delay   Offset      Disp
--------------------+-----+----+-----+------+------+------+-------+----------+-----------
*    198.206.181.70    4    0     2    895    1024   377     0.167   0.323       0.016
=    198.206.181.123   4    0     16   591    1024   377     0.000   0.000       0.000
```

output definitions

Mode	"+" indicates an active peer "-" indicates a pasive peer "=" indicates a client "*" indicates current system peer "^" indicates a broadcast server "`" indicates a broadcast client
IP Address	The server IP address.
Ver	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server, or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.
St	The stratum of the server.
When	Number of seconds passed since last response from remote host.
Poll	Polling interval to the remote host in seconds.

output definitions

Reach	This is a shift register used to determine the reachability status of this peer. This register is displayed to the user in octal values instead of binary, decimal or even hex. The maximum value of an eight-bit binary number is 11111111, which is 377 in octal.
Delay	The delay received from the server in its timestamp.
Offset	The offset received from the server in its timestamp.
Disp	The dispersion value received from the server in its timestamp.

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; When, Poll, Reach fields added.

Related Command

ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpPeerListTable
```

show ntp server client-list

Displays the information about the current NTP clients connected to the server.

show ntp server client-list

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display the tabular information on the current NTP client connected to the server (switch).

Examples

```
-> show ntp server client-list
IP Address           Ver       Key
------------------+-------+----------
172.23.0.201         4          0
10.255.24.121        4          0
```

output definitions

IP Address	The client IP address.
Ver	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.

Release History

Release 7.1.1; command was introduced.

Related Command

show ntp status	Displays information about the current client NTP configuration
ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpClientListTable
   alaNtpPeerListAddress
   alaNtpPeerVersion
   alaNtpPeerAuth
```

show ntp server status

Displays the basic server information for a specific NTP server or a list of NTP servers.

show ntp server status [*ip_address***]**

Syntax Definitions

ip_address	The IP address of the NTP server to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command displays information on the status of any or all configured NTP servers/peers.
- To display a specific server, enter the command with the server's IP address. To display all servers, enter the command with no server IP address.

Examples

```
-> show ntp server status
IP address         = clock3.ovcirrus.com [123.108.200.124],
Host mode          = client,
Peer mode          = server,
Prefer             = no,
Version            = 4,
Key                = 0,
Stratum            = 2,
Minpoll            = 6 (64 seconds),
Maxpoll            = 10 (1024 seconds),
Poll               = 1024 seconds,
when               = 283 seconds,
Delay              = 0.016 seconds,
Offset             = -180.232 seconds,
Dispersion         = 7.945 seconds
Root distance      = 0.026,
Precision          = -14,
Reference IP       = 209.81.9.7,
Status             = configured : reachable : rejected,
Uptime count       = 1742 seconds,
Reachability       = 1,
Unreachable count  = 0,
Stats reset count  = 1680 seconds,
Packets sent       = 1,
Packets received   = 1,
Duplicate packets  = 0,
Bogus origin       = 0,
Bad authentication = 0,
```

```
Bad dispersion     = 0,

-> show ntp server status 198.206.181.139
IP address         = 198.206.181.139,
Host mode          = client,
Peer mode          = server,
Prefer             = no,
Version            = 4,
Key                = 0,
Stratum            = 2,
Minpoll            = 6 (64 seconds),
Maxpoll            = 10 (1024 seconds),
Poll               = 1024 seconds,
when               = 283 seconds,
Delay              = 0.016 seconds,
Offset             = -180.232 seconds,
Dispersion         = 7.945 seconds
Root distance      = 0.026,
Precision          = -14,
Reference IP       = 209.81.9.7,
Status             = configured : reachable : rejected,
Uptime count       = 1742 seconds,
Reachability       = 1,
Unreachable count  = 0,
Stats reset count  = 1680 seconds,
Packets sent       = 1,
Packets received   = 1,
Duplicate packets  = 0,
Bogus origin       = 0,
Bad authentication = 0,
Bad dispersion     = 0,
Last Event         = peer changed to reachable,
```

output definitions

IP address	The server IP address.
Host mode	The host mode of this remote association.
Peer mode	The peer mode of this remote association.
Prefer	Whether this server is a preferred server or not. A preferred server is used to synchronize the client before a non-preferred server.
Version	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server, or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.
Stratum	The stratum of the server. The stratum number is the number of hops from a UTC time source.
Minpoll	The minimum poll time. The client will poll the server for a time update every time this limit has been exceeded.
Maxpoll	The maximum poll time.
When	Number of seconds passed since last response from remote host.
Poll	Polling interval to the remote host in seconds.
Delay	The delay received from the server in its timestamp.

output definitions (continued)

Offset	The offset received from the server in its timestamp.
Dispersion	The dispersion value received from the server in its timestamp.
Root distance	The total round trip delay (in seconds) to the primary reference source.
Precision	The advertised precision of this association.
Reference IP	The IP address identifying the peer's primary reference source.
Status	The peer selection and association status.
Uptime count	The time period (in seconds) during which the local NTP server was associated with the switch.
Reachability	The reachability status of the peer.
Unreachable count	Number of times the NTP entity was unreachable.
Stats reset count	The time delay (in seconds) since the last time the local NTP server was restarted.
Packets sent	Number of packets sent.
Packets received	Number of packets received.
Duplicate packets	Number of duplicated packets received.
Bogus origin	Number of bogus packets.
Bad authentication	Number of NTP packets rejected for not meeting the authentication standards.
Bad dispersion	Number of bad dispersions.
Last Event	The last event.

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; when and poll fields added.

Related Command

ntp client	Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpPeerListTable
   alaNtpPeerShowStatus
```

show ntp keys

Displays information about all authentication keys.

show ntp keys

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command displays the information on the current set of trusted authentication keys.

Examples

```
-> show ntp keys
Key       Status
=======+============
1        untrusted
2        untrusted
3        trusted
4        trusted
5        untrusted
6        untrusted
7        trusted
8        trusted
```

output definitions

Key	The key number corresponding to a key in the key file.
Status	Whether the key is trusted or untrusted.

Release History

Release 7.1.1; command was introduced.

Related Command

ntp key	Labels the specified authentication key identification as trusted or untrusted.
ntp key load	Loads the current key file into memory.

MIB Objects

```
alaNtpAccessKeyIdTable
```

show ntp peers

Displays the information about the current status on the NTP peer association.

show ntp peers

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use this command to display the tabular information on the current NTP peer association status.

Examples

```
-> show ntp peers
IP Address     Ver   Key   St   When   Poll   Reach   Delay    Offset    Disp
---------------+-----+-----+----+------+------+-------+--------+--------+-------
172.23.0.202    4    0     3    895    1024   377     0.300    0.404    0.0024
10.255.24.120   4    0     3    591    1024   377     0.016    0.250    0.0017
```

output definitions

IP Address	Peer IP Address
Ver	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.
St	The stratum of the server.
When	Number of seconds passed since last response from remote host.
Poll	Polling interval to the remote host in seconds.
Reach	This is a shift register used to determine the reachability status of this peer. This register is displayed to the user in octal values instead of binary, decimal or even hex. The maximum value of an eight-bit binary number is 11111111, which is 377 in octal.
Delay	The delay received from the server in its timestamp.
Offset	The offset received from the server in its timestamp.
Disp	The dispersion value received from the server in its timestamp.

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; When, Poll, Reach fields added.

Related Command

ntp client	Enables or disables NTP operation on the switch.
show ntp status	Displays the information about the current NTP status.
show ntp server status	Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

```
alaNtpPeerListTable
   alaNtpPeerListAddress
   alaNtpPeerVersion
   alaNtpPeerAuth
   alaNtpPeerStratum
   alaNtpPeerListDelay
   alaNtpPeerShowOffset
   alaNtpPeerListDispersion
```

show ntp server disabled-interfaces

Displays the ip addresses of the interfaces on which NTP server is not enabled.

show ntp server disabled-interfaces

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command displays ip interfaces on which currently NTP server functionality is disabled.

Examples

```
-> show ntp server disabled-interfaces
IP Address
--------------
172.23.0.202
10.255.24.120
```

output definitions

IP Address	Peer IP Address

Release History

Release 7.1.1; command was introduced.

Related Command

show ntp status	Displays the information about the current NTP status.
show ntp server status	Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

```
alaNtpAccessRestrictedTable
   alaNtpPeerListAddress
```

61 Session Management Commands

Session Management commands are used to monitor and configure operator sessions including FTP, Telnet, HTTP (WebView), console, Secure Shell, and Secure Shell FTP on the switch. (See the SNMP Commands chapter for SNMP session commands.) Maximum number of concurrent sessions allowed:

	OmniSwitch
Telnet(v4)	6
FTP(v4)	**4**
SSH + SFTP(v4)	8
HTTP	**4**

MIB information for commands in this chapter are as follows:

Filename: ALCATEL-IND1-SESSION-MGR-MIB.mib
Module: alcatelIND1SessionMgrMIB

Filename: ALCATEL-IND1-SYSTEM-MIB.mib
Module: alcatelIND1SystemMIB

Filename: ALCATEL-IND1-IP-MIB.mib
Module: alcatelIND1IPMIB

A summary of the available commands is listed here:

session login-attempt
session login-timeout
session banner
session timeout
session prompt
session xon-xoff
show prefix
user profile save
user profile reset
history
command-log
kill
exit
who
whoami
show session config
show session xon-xoff
more
telnet
ssh
ssh login-grace-time
ssh enforce-pubkey-auth
ssh strong-ciphers
ssh strong-hmacs
installsshkey
revokesshkey
show command-log status
show telnet
show ssh

session login-attempt

Sets or resets the number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.

session login-attempt *integer*

Syntax Definitions

integer	The number of times the user can attempt to log in to the switch before the TCP connection is closed. Valid range is 1 to 10.

Defaults

Default is 3 login attempts.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> session login-attempt 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, and default prompt value.
session login-timeout	Sets or resets the amount of time the user can take to accomplish a successful login to the switch.
session timeout	Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

MIB Objects

```
sessionMgr
   sessionLoginAttempt
```

session login-timeout

Sets or resets the amount of time the user can take to accomplish a successful login to the switch. If the timeout period is exceeded, the TCP connection is closed by the switch.

session login-timeout *seconds*

Syntax Definitions

seconds	The number of seconds the switch allows for the user to accomplish a successful login. Valid range is from 5 to 600 seconds.

Defaults

Login timeout default is 55 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> session login-timeout 30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, default prompt value, login timer, and login attempt number.
session login-attempt	Sets or resets the number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.
session timeout	Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

MIB Objects

```
sessionMgr
   sessionLoginTimeout
```

session banner

Sets or resets the file name of the user–defined banner. The banner is a welcome banner that appears after the user sucessfully logs onto the switch.

session {cli | ftp | http} banner *file_name*

no session {cli | ftp | http} banner

Syntax Definitions

cli	Creates/modifies the CLI banner file name.
ftp	Creates/modifies the FTP banner file name.
http	Creates/modifies the HTTP banner file name.
file_name	Banner file name including the path from the switch's /flash directory. The maximum length of the filename and path is 255 characters.

Defaults

- A default banner is included in one of the switch's image files. It is automatically displayed at login so no configuration is needed.
- The user has the option of defining a custom supplementary banner or of using the default banner.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **no session banner** command is used to disable a user defined session banner file from displaying when you log onto the switch.
- The **session banner** command is used to configure or modify the banner file *name*. You must use a text editor to edit the file containing the banner text.

Examples

```
-> session cli banner /switch/banner.txt
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, and default prompt value.

MIB Objects

```
SessionConfigTable
   SessionType
   SessionBannerFileName
```

session timeout

Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

session {cli | http | ftp} timeout *minutes*

Syntax Definitions

cli	Sets the inactivity timeout for CLI sessions.
http	Sets the inactivity timeout for HTTP sessions.
ftp	Sets the inactivity timeout for FTP sessions.
minutes	Inactivity timeout value (in minutes). Valid range 1 to 596523.

Defaults

parameter	default
minutes	4

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The inactivity timer value may be different for each type of interface, such as CLI (Console, Telnet), HTTP (including WebView), and FTP.
- If you change the timer, the new value does not affect current sessions; the new timer is applied to new sessions only.

Examples

```
-> session cli timeout 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show session config	Displays Session Manager information, such as banner file name, session timeout value, and default prompt value.

MIB Objects

```
SessionConfigTable
   SessionType
   SessionInactivityTimerValue
```

session prompt

Configures the default CLI prompt for console and Telnet sessions. The prompt is the symbol and/or text that appears on the screen in front of the cursor.

session prompt default [*string*]

Syntax Definitions

string	Prompt string. Maximum length 31 characters.

Defaults

parameter	default
string	->

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The new prompt will not take effect until you log off and back onto the switch.

Examples

```
-> session prompt default -->
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show session config	Displays Session Manager information such as banner file name, session timeout value, and default prompt value.

MIB Objects

```
SessionConfigTable
   SessionType
   sessionDefaultPromptString
```

session xon-xoff

Enables/disables the XON-XOFF protocol on the console port.

session xon-xoff {enable | disable}

Syntax Definitions

enable	Enables XON-XOFF on the console port.
disable	Disables XON-XOFF on the console port.

Defaults

parameter	default
enable | **disable**	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The switch may interpret noise from an RS232 line as Control-S (XOFF). If the **session console xon-xoff** command is enabled, traffic to the console port may be stopped.

Examples

```
-> session xon-xoff enable
-> session xon-xoff disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show session xon-xoff	Displays whether the console port is enabled or disabled for XON-XOFF.

MIB Objects

```
sessionXonXoffEnable
```

show prefix

Shows the command prefix (if any) currently stored by the CLI. Prefixes are stored for command families that support the prefix recognition feature.

show prefix

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Prefixes are stored for command families that support the prefix recognition feature. These command families include AAA, Interface, Link Aggregation, QoS, Spanning Tree, and VLAN Management. Other command families do not store a prefix.

Examples

```
-> show prefix
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show prefix	This command defines the format of the CLI prompt. The prompt can be defined to include the command prefix.

MIB Objects

N/A

user profile save

Saves the user account settings for prompts and the more mode screen setting. These settings will be automatically loaded when the user account logs on.

user profile save

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to save prompt definitions and more mode screen settings for use in future login sessions for the current user account.
- Use the **user profile reset** command to set values to their factory defaults.

Examples

```
-> user profile save
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show prefix	Defines substitute command text for the switch's CLI command keywords.
user profile reset	Resets the alias, prompt and more values to their factory defaults.

MIB Objects

N/A

user profile reset

Resets the alias, prompt, and more values to their factory defaults.

user profile reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> user profile reset
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show prefix	Defines substitute command text for the switch's CLI command keywords.
user profile save	Saves the user account settings for aliases, prompts and the more screen.

MIB Objects

N/A

history

Displays commands that you have recently issued to the switch. The commands are displayed in a numbered list.

history *number*

Syntax Definitions

number	The number of commands to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> history
1 show cmm
2 show fan
3 show sensor
```

output definitions

Index	The index of the commands for this CLI session and the associated command.

Release History

Release 7.1.1; command was introduced.

Related Commands

!	Recalls commands listed in the history buffer and displays them at the CLI prompt.

MIB Objects

N/A

!

Recalls commands listed in the history buffer and displays them at the CLI prompt.

!{! | *n*}

Syntax Definitions

!	Recalls the last command listed in the history buffer and displays that command at the CLI prompt.
n	Identifies a single command in the history buffer by number and displays that command at the CLI prompt.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You can use the **history** command to list all commands in the history buffer, then use the **!*n*** syntax to issue a single command from the list.
- When you use **!*n*** or **!!** to recall a command in the history buffer list, you must press the Enter key to execute the command.

Examples

```
-> history
1* show ip interface
2 show vlan
3 show arp
4 clear arp
->!2
show vlan
 vlan  type  admin  oper  ip   mtu   name
-----+------+-----+-----+-----+-----+------------
   1   std    Ena   Ena   Dis  1500   VLAN 1
  10   std    Ena   Ena   Ena  1500   VLAN 10
  12   std    Ena   Ena   Ena  1500   VLAN 12
  14   std    Ena   Ena   Ena  1500   VLAN 14
  30   vip    Ena   Ena   Ena  1500   VIP VLAN 30
  40   vip    Ena   Ena   Ena  1500   VIP VLAN 40
4094   mcm    Ena   Ena   Dis  9198   MCM IPC
```

Release History

Release 7.1.1; command was introduced.

Related Commands

history	Sets the number of commands that will be stored in the CLI history buffer.

MIB Objects

N/A

command-log

Enables or disables command logging on the switch. When command logging is enabled, a **command.log** is automatically created; this file stores a comprehensive CLI command history for all active sessions since the function was *first* enabled.

command-log {enable | disable}

Syntax Definitions

enable	Creates a file called **command.log** in the switch's **/flash** directory. Any configuration commands entered on the command line will be recorded to this file until command logging is disabled.
disable	Disables logging of current session commands to the **command.log** file.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The maximum log file size is 66,402 bytes; the file may hold up to 100 commands.

Examples

```
-> command-log enable
-> command-log disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show command-log	Displays the contents of the **command.log** file.
show command-log status	Shows the current status of the command logging function (i.e., enabled or disabled).

MIB Objects

```
sessionCliCommandLogEnable
```

kill

Kills an active session. The command takes effect immediately.

kill *session_number*

Syntax Definitions

session_number	Number of the session you want to kill.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **who** command to obtain the session number variable.
- You cannot kill your own session.
- You cannot kill a connected session where the user has not yet completed the login process. These sessions appear with username “(at login)” when displayed with the **who** command.

Examples

```
-> kill 3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

who	Displays all active login sessions (e.g., Console, Telnet, FTP, HTTP)

MIB Objects

```
SessionMgr
   sessionIndex
   sessionRowStatus
```

exit

Ends the current CLI session. If the CLI session to the switch was via Telnet, the connection is closed.

exit

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> exit
```

Release History

Release 7.1.1; command was introduced.

Related Commands

kill	Kills an active session. The command takes effect immediately.

MIB Objects

```
SessionMgr
   sessionIndex
   sessionRowStatus
```

whoami

Displays the current user session.

whoami

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the **who** command to display all sessions on the switch.

Examples

```
-> whoami
Session number = 5
  User name   = admin,
  Access type = telnet,
  Access port = NI,
  IP address  = 121.251.17.76,
  Read-only domains   = None,
  Read-only families  = ,
  Read-Write domains  = All ,
  Read-Write families = ,
```

output definitions

Session Number	The session number assigned to the user.
User name	User name.
Access type	Type of access protocol used to connect to the switch.
Access port	Switch port used for access during this session.
Ip Address	User IP address.
Read-only domains	The command domains available with the user's read-only access.
Read-only families	The command families available with the user's read-only access.
Read-Write domains	The command domains available with the user's read-write access.
Read-Write families	The command families available with the user's read-write access.

Release History

Release 7.1.1; command was introduced.

Related Commands

who	Displays all active login sessions (e.g., Console, Telnet, FTP, HTTP).
kill	Kills another user's session.

MIB Objects

```
SessionActive
   sessionIndex
   sessionAccessType
   sessionPhysicalPort
   sessionUserName
   sessionUserReadPrivileges
   sessionUserWritePrivileges
   sessionUserProfileNumber
   sessionUserIpAddress
   sessionRowStatus
```

who

Displays all active login sessions.

who

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You can identify your current login session by using the IP address.
- This command applies to the following session types: Console, Telnet, SSH, FTP, SFTP, HTTP, HTTPS, SNMP.

Examples

```
-> who
Session number = 0
  User name   = (at login),
  Access type = console,
  Access port = Local,
  IP address  = 0.0.0.0,
  Read-only domains   = None,
  Read-only families  = ,
  Read-Write domains  = None,
  Read-Write families = ,

Session number = 5
  User name   = admin,
  Access type = telnet,
  Access port = NI,
  IP address  = 128.251.17.176,
  Read-only domains   = None,
  Read-only families  = ,
  Read-Write domains  = All ,
  Read-Write families = ,
```

output definitions

Session Number	The session number assigned to the user.
User name	User name.
Access type	Type of access protocol used to connect to the switch.

output definitions (continued)

Access port	Switch port used for access during this session.
Ip Address	User IP address.
Read-only domains	The command domains available with the user's read-only access.
Read-only families	The command families available with the user's read-only access.
Read-Write domains	The command domains available with the user's read-write access.
Read-Write families	The command families available with the user's read-write access.

Possible values for command domains and families are listed here:

Release History

Release 7.1.1; command was introduced.

Related Commands

whoami	Displays current user session.
kill	Kills another user's session.

MIB Objects

```
SessionActive
   sessionIndex
   sessionAccessType
   sessionPhysicalPort
   sessionUserName
   sessionUserReadPrivileges
   sessionUserWritePrivileges
   sessionUserProfileNumber
   sessionUserIpAddress
   sessionRowStatus
```

show session config

Displays session manager configuration information (e.g., default prompt, banner file name, inactivity timer, login timer, and login attempts).

show session config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Use the configuration commands detailed in this section to modify any of the values displayed.

Examples

```
-> show session config

Cli Default Prompt              = ->
Cli Banner File Name            = ,
Cli Inactivity Timer in minutes  = 60
Ftp Banner File Name            = ,
Ftp Inactivity Timer in minutes  = 60
Http Inactivity Timer in minutes = 60
Login Timer in seconds          = 60
Maximum number of Login Attempts = 2
```

output definitions

Cli Default Prompt	Default prompt displayed for CLI sessions.
Cli Banner File Name	Name of the file that contains the banner information that will appear during a CLI session.
Cli Inactivity Timer in minutes	Inactivity timer value (in minutes) for CLI sessions. The user is logged off when this value is exceeded.
Ftp Banner File Name	Name of the file that contains the banner information that will appear during an FTP session.
Ftp Inactivity Timer in minutes	Inactivity timer value (in minutes) for FTP sessions. The user is logged off when this value is exceeded.
Http Inactivity Timer in minutes	Inactivity timer value (in minutes) for HTTP (including WebView) sessions. The user is logged off when this value is exceeded.

output definitions (continued)

Login Timer in seconds	The amount of time the user can take to accomplish a successful login to the switch. If the timeout period is exceeded, the TCP connection is closed by the switch.
Maximum number of Login Attempts	The number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.

Release History

Release 7.1.1; command was introduced.

Related Commands

session prompt	Configures the default CLI prompt for console and Telnet sessions.
session banner	Sets the file name of the user–defined banner.
session timeout	Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface.
session login-attempt	Sets the number of times a user can attempt to log into the switch unsuccessfully before the TCP connection is closed.
session login-timeout	Sets the amount of time the user can take to accomplish a successful login to the switch.

MIB Objects

```
SessionConfigTable
   sessionType
   sessionBannerFileName
   sessionInactivityTimerValue
   sessionDefaultPromptString
```

show session xon-xoff

Displays whether the console port is enabled or disabled for XON-XOFF.

show session xon-xoff

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The switch may interpret noise from an RS232 line as Control-S (XOFF). If the console port is enabled for XON-XOFF (through the **session xon-xoff** command), traffic to the console port may be stopped.

Examples

```
-> show session xon-xoff
XON-XOFF Enabled
```

Release History

Release 7.1.1; command was introduced.

Related Commands

session xon-xoff	Enables/disables the XON-XOFF protocol on the console port.

MIB Objects

```
sessionXonXoffEnable
```

more

Enables the more mode for your console screen display.

more *filename*

Syntax Definitions

filename	The file to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This parameter can also be used to pipe output from the CLI.
- This command is case sensitive.

Examples

```
-> more textfile.txt
-> write terminal | more
```

Release History

Release 7.1.1; command was introduced.

Related Commands

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

telnet

Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.

[vrf *name***] telnet {port** [**default** | *service_port*] | **admin-state** [**enable** | **disable**] | *ip_address***}**

Syntax Definitions

name	Name of the VRF.
default	Sets the port back to the default of 23.
service_port	The TCP service port number. Must be 23 or between 20000-20999.
enable | **disable**	Enables or disables telnet access.
ip_address	Specifies the IPv4 or IPv6 address for the Telnet session.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The default directory for Telnet is **/flash**.

Examples

```
-> telnet port 20999
-> telnet admin-state disable
-> telnet 172.17.6.228
-> vrf vrf1 telnet admin-state enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

ssh	Invokes the Secure Shell on the switch. A Secure Shell is used to make a secured connection to a remote system or device.
show telnet	Displays the current configuration specifying the ports the telnet daemons are listening on.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
   alaIpTelnetAdminStatus
```

ssh

Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.

[vrf *name***] ssh {port** [**default |** *service_port*] **| admin-state** [**enable | disable**] | *ip_address***}**

Syntax Definitions

name	Name of the VRF.
default	Sets the port back to the default of 22.
service_port	The TCP service port number. Must be 23 or between 20000-20999.
**enable	disable**	Enables or disables Secure Shell.
ip_address	Specifies the IPv4 or IPv6 address for the Secure Shell.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

You must have a valid username and password for the specified host.

Examples

```
-> ssh port 20000
-> ssh admin-state disable
-> ssh 172.155.11.211
login as:

-> vrf vrf1 ssh admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

telnet	Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.
ssh enforce-pubkey-auth	Invokes Secure Shellv6 on the switch. Secure Shellv6 is used to make a secured connection to an SSHv6 server.
show command-log	Displays the status of Secure Shell, SCP/SFTP on the switch.
show ssh	Displays the current configuration specifying the ports SSH daemons are listening on.

MIB Objects

```
alaIpSshConfig
   alaIpSshAdminStatus
   alaIpSshPort
```

ssh login-grace-time

Configures the duration in which the user has to enter a login password and authenticate for an SSH session.

ssh login-grace-time *seconds*

Syntax Definitions

seconds	The number of seconds for the grace time period. The range is 30–600.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

By default, the login grace time period is set to 120 seconds.

Examples

```
-> ssh login-grace-time 300
-> ssh login-grace-time 600
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ssh	Displays the current SSH configuration for the switch.

MIB Objects

```
alaIpSshConfig
   alaIpSshLoginGraceTime
```

ssh enforce-pubkey-auth

Enables or disables Secure Shell public key and password authentication. When enabled, password authentication is not allowed.

ssh enforce-pubkey-auth {enable | disable}

Syntax Definitions

enable	Enforces only SSH public key authentication.
disable	Enforces both SSH public key and password authentication.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ssh enforce-pubkey-auth enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

telnet	Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.

MIB Objects

```
alaIpSshConfig
   alaIpSshPubKeyEnforceAdminStatus
```

ssh strong-ciphers

Enables or disables the enforcement of a Secure Shell (SSH) cipher configuration across a switch reboot.

ssh strong-ciphers {enable | disable}

Syntax Definitions

enable	Enables the enforcement of an SSH cipher configuration.
disable	Disables the enforcement of an SSH cipher configuration.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> ssh strong-ciphers enable
-> ssh strong-ciphers disable
```

Release History

Release 8.3.1; command was introduced.

Related Commands

show ssh	Displays the current SSH configuration for the switch.

MIB Objects

```
alaIpSshConfig
   alaIpSshStrongCiphersAdminStatus
```

ssh strong-hmacs

Enables or disables the enforcement of a Secure Shell (SSH) HMAC configuration across a switch reboot.

ssh strong-hmacs {enable | disable}

Syntax Definitions

enable	Enables the enforcement of an HMAC configuration.
disable	Disables the enforcement of an HMAC configuration.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- SSH HMAC refers to message authentication codes that use cryptographic hash functions.
- Enable strong-hmacs will enforce the use of *"hmac-sha1 , hmac-sha2-256, hmac-sha2-512*" in ssh server.
- Disable will select default hmacs in the configuration.

Examples

```
-> ssh strong-hmacs enable
-> ssh strong-hmacs disable
```

Release History

Release 8.3.1; command was introduced.

Related Commands

show ssh	Displays the current SSH configuration for the switch.

MIB Objects

```
alaIpSshConfig
   alaIpSshStrongHmacsAdminStatus
```

installsshkey

Used to install the public key used for SSH onto the switch.

installsshkey *user path*

Syntax Definitions

user	The user that the key will be associated with.
path	The location of the key file.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Be sure the associated private key is stored on the client device.
- Verify that the user that will use SSH is a valid user name on the OmniSwitch.
- Refer to the Switch Management Guide for information on generating the public/private keys.

Examples

```
-> installsshkey new_ssh_user /flash/system/new_ssh_user_rsa.pub
```

Release History

Release 8.3.1; command was introduced.

Related Commands

revokesshkey	Used to revoke a key from an SSH user.
show ssh	Displays the current SSH configuration for the switch.

MIB Objects

N/A

revokesshkey

Used to revoke a key from an SSH user.

revokesshkey *user remote-user*

Syntax Definitions

user	The local user name.
remote-user	The user on the remote client device.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> revokesshkey new_ssh_user remote_ssh_user@192.168.10.1
```

Release History

Release 8.3.1; command was introduced.

Related Commands

installsshkey	Used to install the public key used for SSH onto the switch.
show ssh	Displays the current SSH configuration for the switch.

MIB Objects

N/A

show command-log

Displays the contents of the **command.log** file. This file contains a record of all CLI commands executed on the switch since the command logging function was enabled. For more information on enabling and disabling command logging, refer to page 61-16.

show command-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The most recent commands are listed first.
- The command history is archived to the **command.log** file. If this file is removed, the command history will no longer be available. In addition, the **command.log** file has a 66,402 byte capacity. This capacity allows up to 100 commands; if the maximum capacity is reached, only the 100 most recent commands display.

Examples

```
-> show command-log
Command : ip interface Marketing address 17.11.5.2 vlan 255
  UserName : admin
  Date     : FRI JAN 09 00:20:01
  Ip Addr  : 128.251.19.240
  Result   : SUCCESS

Command : ip interface "Distribution" 11.255.14.102 vlan 500 local-proxy-arp
  UserName : admin
  Date     : FRI JAN 09 00:19:44
  Ip Addr  : 128.251.19.240
  Result   : ERROR: Ip Address must not belong to IP VLAN 44 subnet

Command : command-log enable
  UserName : admin
  Date     : FRI JAN 09 00:18:49
  Ip Addr  : 128.251.19.240
  Result   : SUCCESS
```

output definitions

Command	The exact syntax of the command, as entered by the user.
UserName	The name of the user session that entered the command. For more information on different user session names, refer to the **user** command on page 38-56, or the "Managing Switch User Accounts" chapter in the *OmniSwitch AOS Release 8 Switch Management Guide*.
Date	The date and time, down to the second, when the command was entered.
IpAddr	The IP address of the terminal from which the command was entered.
Result	The outcome of the command entry. Options include **SUCCESS** and **ERROR**. For erroneous command entries, the same error details presented by the switch at the time the command was entered are also displayed in the log file.

Release History

Release 7.1.1; command was introduced.

Related Commands

command-log	Enables or disables command logging on the switch.
show command-log status	Shows the current status of the command logging function (i.e., enabled or disabled).

MIB Objects

```
sessionCliCommandLogEnable
```

show command-log status

Shows the current status of the command logging function (i.e., enabled or disabled).

show command-log status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show command-log status
CLI command logging : Enable
```

output definitions

CLI command logging	The current status of command logging on the switch. Options include **Disable** and **Enable**.

Release History

Release 7.1.1; command was introduced.

Related Commands

command-log	Enables or disables command logging on the switch.

MIB Objects

```
sessionCliCommandLogStatus
```

show telnet

Displays the current configuration specifying the ports the telnet daemons are listening on.

[vrf *name***] show telnet**

Syntax Definitions

name	Name of the VRF.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If VRF is specified, the current status of the telnet daemon for the specified VRF is displayed.

Examples

```
vrf1::-> show telnet
Telnet Admin-State = Enabled
Telnet Port = 23
```

Release History

Release 7.1.1; command was introduced.

Related Commands

command-log	Enables or disables command logging on the switch.

MIB Objects

```
alaIpTelnetAdminStatus
alaIpTelnetPort
```

show ssh

Displays the current configuration specifying the ports on which the SSH daemons are listening.

[vrf *name***] show ssh**

Syntax Definitions

name	Name of the VRF.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If VRF is specified, the current status of the SSH daemon for the specified VRF is displayed.

Examples

```
vrf1::-> show ssh
Ssh Admin-State = Enabled
Ssh Port = 22
Ssh Enforce-Pubkey-Auth = Disabled
Ssh Strong-Ciphers = Disabled
Ssh Strong-Hmacs = Disabled
Ssh login-grace-time = 600 seconds
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; **Ssh Strong-Ciphers** and **Ssh Strong-Hmacs** fields added.
Release 8.3.1.R02; **Ssh login-grace-time** field added.

Related Commands

command-log	Enables or disables command logging on the switch.

MIB Objects

```
alaIpSshConfig
   alaIpSshAdminStatus
   alaIpSshPort
   alaIpSshPubKeyEnforceAdminStatus
   alaIpSshStrongCiphersAdminStatus
   alaIpSshStrongHmacsAdminStatus
   alaIpSshLoginGraceTime
```

62 File Management Commands

This chapter includes descriptions for CLI commands used to manage files on the switch. Several of these commands are used to create, move, and delete both files and directories in the OmniSwitch flash directory. Other commands allow you to change command privileges and to monitor the memory usage on the switch.

MIB information for the system commands is listed here:

Filename: ALCATEL-IND1-SYSTEM-MIB.mib
Module: alcatelIND1SystemMIB

Filename: ALCATEL-IND1-CHASSIS-MIB.mib
Module: alcatelIND1ChassisMIB

A summary of the available commands is listed here:

File System	**cd** **pwd** **mkdir** **rmdir** **ls** **rm** **cp** **scp** **mv** **chmod** **freespace** **fsck** **newfs**
System Services	**vi** **tty** **show tty** **tftp** **sftp** **ftp** **show ftp**

cd

Changes the current working directory of the switch.

cd [*path***]**

Syntax Definitions

path	Specifies the path to the working directory. If no path is specified, the current directory of the switch is changed to the higher directory level.

Defaults

The default working directory of the switch is **/flash**.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Separate the multiple directory names that are part of the path with a slash (/).

Examples

```
-> cd
-> cd /flash/certified
```

Release History

Release 7.1.1; command introduced.

Related Commands

pwd	Displays the current working directory of the switch.
mkdir	Creates a new directory.
rmdir	Deletes an existing directory.
ls	Displays the contents of a specified directory or the current working directory.
rm	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesWorkingDirectory
```

pwd

Displays the current working directory of the switch.

pwd

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The **pwd** command can also be used on the secondary CMM.

Examples

```
-> pwd
/flash
```

Release History

Release 7.1.1; command introduced.

Related Commands

cd	Changes the current working directory of the switch.
mkdir	Creates a new directory.
rmdir	Deletes an existing directory.
ls	Displays the contents of a specified directory or the current working directory.
rm	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesWorkingDirectory
```

mkdir

Creates a new directory.

mkdir [*options***] [***path***]** */dirname*

Syntax Definitions

options	Use the '?' on the command line for a list of options.
path	The path or location in which the new directory is to be created. If no path name is specified, the new directory is created in the current directory.
dirname	A user-defined name for the new directory.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Separate the directory names that are part of the path with a slash (/). Refer to the examples below.
- The **mkdir** command can also be used on the secondary CMM.

Examples

```
-> mkdir test_directory
-> mkdir flash/test_directory
-> mkdir
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.

Usage: mkdir [OPTIONS] DIRECTORY...

Create DIRECTORY

Options:
        -m      Mode
        -p      No error if exists; make parent directories as needed
```

Release History

Release 7.1.1; command introduced.

Related Commands

cd	Changes the current working directory of the switch.
pwd	Displays the current working directory of the switch.
rmdir	Deletes an existing directory.
ls	Displays the contents of a specified directory or the current working directory.
rm	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

rmdir

Deletes an existing directory.

rmdir [*options***]** *dirname*

Syntax Definitions

options	Use the '?' on the command line for a list of options.
dirname	The name of the existing directory to be removed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Separate the directory names that are part of the path with a slash (/). Refer to the examples below.
- This command can also be used on the secondary CMM.

Examples

```
-> rmdir ./working
-> rmdir flash/working
-> rmdir ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.

Usage: rmdir [OPTIONS] DIRECTORY...

Remove DIRECTORY if it is empty

Options:
        -p|--parents    Include parents
        --ignore-fail-on-non-empty
```

Release History

Release 7.1.1; command introduced.

Related Commands

cd	Changes the current working directory of the switch.
pwd	Displays the current working directory of the switch.
mkdir	Creates a new directory.
ls	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

ls

Displays the contents of a specified directory or the current working directory.

ls [*options***] [***path/filename***]**

Syntax Definitions

options	Use the '?' on the command line for a list of options.
filename	Specifies the file or directory path.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Separate the multiple directory names that are part of the path with a slash (/).

Examples

```
-> ls
-> ls -l /flash/certified
-> ls ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.

Usage: ls [-1AacCdeFilnpLRrSsTtuvwxXhk] [FILE]...

List directory contents

Options:
        -1      List in a single column
        -A      Don't list . and ..
        -a      Don't hide entries starting with .
        -C      List by columns
        -c      With -l: sort by ctime
        --color[={always,never,auto}]   Control coloring
        -d      List directory entries instead of contents
        -e      List full date and time
        -F      Append indicator (one of */=@|) to entries
        -i      List inode numbers
        -l      Long listing format
        -n      List numeric UIDs and GIDs instead of names
        -p      Append indicator (one of /=@|) to entries
        -L      List entries pointed to by symlinks
        -R      Recurse
        -r      Sort in reverse order
        -S      Sort by file size
        -s      List the size of each file, in blocks
        -T N    Assume tabstop every N columns
```

```
-t      With -l: sort by modification time
-u      With -l: sort by access time
-v      Sort by version
-w N    Assume the terminal is N columns wide
-x      List by lines
-X      Sort by extension
-h      List sizes in human readable format (1K 243M 2G)
```

Release History

Release 7.1.1; command introduced.

Related Commands

cd	Changes the current working directory of the switch.
pwd	Displays the current working directory of the switch.
mkdir	Creates a new directory.
rmdir	Deletes an existing directory.
rm	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

rm

Permanently deletes an existing file.

rm [*options***] [***path/filename***]**

Syntax Definitions

options	Use the '?' on the command line for a list of options.
filename	Specifies the file or directory path.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Separate the multiple directory names that are part of the path with a slash (/). Refer to the examples below.
- Use care when deleting files. Depending on your switch and network configurations, specific configuration and image files must be present for your system to work properly.
- This command can also be used on the secondary CMM.

Examples

```
-> rm test_config_file
-> rm flash/test_config_file
-> rm ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.

Usage: rm [OPTIONS] FILE...

Remove (unlink) FILEs

Options:
        -i      Always prompt before removing
        -f      Never prompt
        -R,-r   Recurse
```

Release History

Release 7.1.1; command introduced.

Related Commands

cp	Copies an existing file or directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

cp

Copies an existing file. This command can also copy a directory if the -r keyword is used.

cp [*options***]** *source destination*

Syntax Definitions

options	Use the '?' on the command line for a list of options.
source	The name of the existing file to be copied.
destination	The new user-defined file name for the resulting file copy. If you are copying a file to the same directory as the original, the file name for the copy must be different from the original.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You should verify that the **/flash** directory of your switch has enough available memory to hold the copies of the files and directories created.
- A file can be copied to a new directory location. Copy of a file can also be created in the same directory that contains the original file.
- Separate the multiple directory names that are part of the path with a slash (/). Refer to the examples below.
- This command can also be used on the secondary CMM.

Examples

```
-> cp flash/snapshots/asc.1.snap flash/snapshot/snapshot_copy
-> cp flash/snapshots/asc.1.snap snapshot_copy
-> cp asc.1.snap flash/snapshot/snapshot_copy
-> cp asc.1.snap snapshot_copy
-> cp ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.

Usage: cp [OPTIONS] SOURCE DEST

Copy SOURCE to DEST, or multiple SOURCE(s) to DIRECTORY

Options:
        -a      Same as -dpR
        -R,-r   Recurse
        -d,-P   Preserve symlinks (default if -R)
        -L      Follow all symlinks
```

```
-H      Follow symlinks on command line
-p      Preserve file attributes if possible
-f      Force overwrite
-i      Prompt before overwrite
-l,-s   Create (sym)links
```

Release History

Release 7.1.1; command introduced.

Related Commands

mv	Moves an existing file or directory to a new location.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

scp

Copies an existing file in a secure manner.

scp [*options***]** *user_name@remote_ip_addr:***[***path/***]***source* **[***path/***]***target*

scp [*options***] [***path/***]***source user_name@remote_ip_addr:***[***path/***]***target*

Syntax Definitions

options	Use the '?' on the command line for a list of options.
user_name@remote_ip_addr:	The username along with the IPv4 or IPv6 address of the remote switch.
path/	Specifies the path containing the file to be copied and the path where the file will be copied.
source	The name of the file(s) to be copied.
target	The new user-defined file name for the resulting file copy.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- This command will prompt you to enter the admin password, and the names and the path of the files being copied will be displayed.
- A file may be copied to a new location; you are not required to copy a file to the same directory that contains the original.
- Separate the multiple directory names that are part of the path with a slash (/). Refer to the examples below.

Examples

```
-> scp admin@172.17.11.13:/flash/working/Kos.img /flash/working/Kos.img
admin's password for keyboard-interactive method:

Fetching /flash/working/Kos.img to /flash/working/Kos.img
Connection to 172.17.11.13 closed.

-> scp /flash/working/Kos.img admin@172.17.11.13:/flash/working/Kos.img
admin's password for keyboard-interactive method:

Uploading /flash/working/Kos.img to /flash/working/Kos.img
Connection to 172.17.11.13 closed.

-> scp admin@172.17.11.13:/flash/working/*.img /flash/working
admin's password for keyboard-interactive method:
```

```
Fetching /flash/working/K2os.img to /flash/working/K2os.img
Fetching /flash/working/Kadvrout.img to /flash/working/Kadvrout.img
Fetching /flash/working/Kbase.img to /flash/working/Kbase.img
Fetching /flash/working/Keni.img to /flash/working/Keni.img
Fetching /flash/working/Kos.img to /flash/working/Kos.img
Fetching /flash/working/Krelease.img to /flash/working/Krelease.img
Fetching /flash/working/Ksecu.img to /flash/working/Ksecu.img
Connection to 172.17.11.13 closed.
-> scp ?
usage: scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
           [-l limit] [-o ssh_option] [-P port] [-S program]
           [[user@]host1:]file1 ... [[user@]host2:]file2
```

Release History

Release 7.1.1; command introduced.

Related Commands

mv	Moves an existing file or directory to a new location.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

mv

Moves an existing file or directory to a new location.

mv [*options***]** *source destination*

Syntax Definitions

options	Use the '?' on the command line for a list of options.
source	The name of the existing file to be copied.
destination	The new user-defined file name for the resulting file copy. If you are copying a file to the same directory as the original, the file name for the copy must be different from the original.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **mv** command does not make a copy of the file or directory being moved. To copy a file or directory to the current path or to a new location, use the **cp** command.
- Separate the directory names and file names that are part of the path with a slash (/). Refer to the examples below.
- This command can also be used on the secondary CMM.

Examples

```
-> mv flash/asc.1.snap flash/backup_files/asc.1.snap
-> mv ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.

Usage: mv [OPTIONS] SOURCE DEST
or: mv [OPTIONS] SOURCE... DIRECTORY

Rename SOURCE to DEST, or move SOURCE(s) to DIRECTORY

Options:
        -f      Don't prompt before overwriting
        -i      Interactive, prompt before overwrite
```

Release History

Release 7.1.1; command introduced.

Related Commands

rm	Renames an existing file or directory.
cp	Copies an existing file or directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

chmod

Changes the write privileges for a specified file.

chmod {+w | -w} [*path/***]***file*

Syntax Definitions

+w	Enables read-write privileges for the file.
-w	Disables write privileges for the file—i.e., the file becomes read-only.
path/	The path containing the file for which privileges are being changed.
file	The name of the file for which read-write privileges are being changed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> chmod +w vlan.config
-> chmod -w flash/backup_configs/vlan.config
```

Release History

Release 7.1.1; command introduced.

Related Commands

freespace	Changes the write privileges for a specified file.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

freespace

Displays the amount of free space available in the **/flash** directory.

freespace [/flash | /uflash]

Syntax Definitions

/flash	The amount of free space is shown for the **/flash** directory.
/uflash	The amount of free space is shown for the **/uflash** directory.

Defaults

N/A

Usage Guidelines

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Examples

```
-> freespace /flash
/flash 3143680 bytes free

-> freespace
/flash 3143680 bytes free
```

Release History

Release 7.1.1; command introduced.

Related Commands

fsck	Performs a file system check, including diagnostic information in the event of file corruption. If the **fsck** command detects a problem with the **/flash** file system, a message is displayed indicating the problem, along with any steps needed to resolve it.

MIB Objects

```
SystemFileSystemTable
   systemFileSystemFreespace
```

fsck

Performs a file system check, including diagnostic information in the event of file corruption.

fsck /uflash {repair | no-repair}

Syntax Definitions

/uflash	Indicates that the file system check will be performed on the **/uflash** directory.
repair	Attempt to repair any problems found.
no-repair	Do not attempt to repair any problems found.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

This command provides the option to automatically repair errors.

Examples

```
-> fsck /uflash repair

/uflash/  - disk check in progress ..
/uflash/  - Volume is OK

          total # of clusters:  14,773
           # of free clusters:  4,132
            # of bad clusters:  0
              total free space:  8,264 Kb
    max contiguous free space:  5,163,008 bytes
                   # of files:  46
                 # of folders:  3
         total bytes in files:  21,229 Kb
             # of lost chains:  0
   total bytes in lost chains:  0
```

Release History

Release 7.1.1; command introduced.

Related Commands

freespace	Displays the amount of free space available in the **/flash** directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

newfs

Deletes the complete **/uflash** file system and all files within it, replacing it with a new, empty **/uflash** file system. Use this command when you want to reload all files in the file system or in the unlikely event that the **/uflash** file system becomes corrupt.

newfs /uflash

Syntax Definitions

/uflash	This indicates that the complete file system will be replaced.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- It is recommended that you preserve all required image and configuration files by saving them to a remote host before executing the **newfs** command.
- Do not power-down the switch after running the **newfs** command until you reload all required image and configuration files.

Examples

```
-> newfs /uflash
```

Release History

Release 7.1.1; command introduced.

Related Commands

N/A

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

vi

Launches the switch's Vi text editor. The Vi file editor allows you to view or edit the contents of a specified text file.

vi [*options***] [***path/***]***filename*

Syntax Definitions

options	Use the '?' on the command line for a list of options.
path/	The path (i.e., location) containing the file being viewed or edited. If no path is specified, the command assumes the current directory.
filename	The name of the existing file being viewed or edited.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Until you exit the switch's file editor, all keystrokes will be passed to the text editor rather than the switch's command line.
- This command can also be used on the secondary CMM.

Examples

```
-> vi test_config_file
-> vi ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.

Usage: vi [OPTIONS] [FILE]...

Edit FILE

Options:
        -c      Initial command to run ($EXINIT also available)
        -R      Read-only
        -H      Short help regarding available features
```

Release History

Release 7.1.1; command introduced.

Related Commands

tty	Displays current TTY settings.

MIB Objects

```
systemServices
   systemServicesTtyLines
   systemServicesTtyColumns
```

tty

Specifies the number of lines and columns to be displayed on the terminal screen while the switch is in the edit file mode.

tty *lines columns*

Syntax Definitions

lines	The number of lines to be displayed on the terminal emulation screen for the current session. Values may range from 10 to 150.
columns	The number of columns to be displayed for each line. One column is the same width as a single text character. Values may range from 20 to 150.

Defaults

parameter	default
lines	24
columns	80

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The number of lines and columns set with this command controls the screen size when the switch is editing or viewing a text file with the **vi** or **tftp** commands.
- The values set with this command do not control the CLI screen when the switch is operating in normal mode.
- This command can also be used on the secondary CMM.

Examples

```
-> tty 10 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show tty	Displays current TTY settings.

MIB Objects

```
systemServices
   systemServicesTtyLines
   systemServicesTtyColumns
```

show tty

Displays current TTY settings.

show tty

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Shows the settings made with the **tty** command.
- This command can also be used on the secondary CMM.

Examples

```
-> show tty
lines = 24, columns = 80
```

Release History

Release 7.1.1; command introduced.

Related Commands

tty	Specifies the number of TTY lines and columns to be displayed.

MIB Objects

```
systemServices
   systemServicesTtyLines
   systemServicesTtyColumns
```

tftp

Starts a TFTP client session that enables a file transfer to an TFTP server.

tftp [*options***] *host* [***port***]**

Syntax Definitions

options	Enter a question mark (?) to get a list of options.
host	Specifies the IP address of the TFTP server.
port	Specifies the port for the TFTP transfer.

Defaults

- If a path is not specified with the filename, the current path is used by default (for example, /flash).
- If a local filename is not specified, the remote filename is used by default.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The OmniSwitch supports TFTP client functionality only.
- A TFTP server has no provisions for user authentication.
- When downloading a file to the switch, the file size must not exceed the available flash space.

Examples

```
-> tftp -g -l local_file -r remote_file 198.51.100.100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

cd	Changes the current working directory of the switch.
pwd	Displays the current working directory of the switch.
ls	Displays the contents of a specified directory or the current working directory.

MIB Objects

N/A

sftp

Starts an SFTP session. An SFTP session provides a secure file transfer method.

sftp [*options***] {***ip_address***}**

Syntax Definitions

options	Enter a question mark (?) to get a list of options.
ip_address	Specifies the IPv4 or IPv6 address for the SFTP session.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You must have a valid username and a password for the specified host.
- After logging in, SFTP commands are supported. Some of these commands are defined in the following table:

cd path	Change remote path to ‘path’.
lcd path	Change local directory to ‘path’.
chmod mode path	Change permissions of file ‘path’ to ‘mode’.
help	Display command help information.
get remote-path [local path]	Download a file from the remote path to the local path.
lls [path]	Display local directory listing.
ln oldpath newpath	Creates a symbolic link (symlink) to the remote file.
symlink oldpath newpath	Creates a symbolic link (symlink) to the remote file.
lmkdir path	Create local directory.
lpwd	Print local working directory.
ls [path]	Display remote directory listing.
mkdir path	Create remote directory.
put local-path [remote-path]	Upload file.
pwd	Display remote working directory.
exit	Quit the sftp mode.
quit	Exit the sftp mode.
rename oldpath newpath	Rename a remote file.

rmdir path	Remove remote directory.
rm path	Delete remote file.
version	Show the current SFTP version.
?	Synonym for help. Displays command help information.

Examples

```
-> sftp 12.251.11.122
login as:
-> sftp
usage: sftp [-1Cv] [-B buffer_size] [-b batchfile] [-F ssh_config]
            [-o ssh_option] [-P sftp_server_path] [-R num_requests]
            [-S program] [-s subsystem | sftp_server] host
       sftp [[user@]host[:file [file]]]
       sftp [[user@]host[:dir[/]]]
       sftp -b batchfile [user@]host
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ftp	Starts an FTP session.
ssh	Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.

MIB Objects

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

ftp

Starts an FTP session.

ftp {port [**default |** *service_port*] | **admin-state [enable | disable] |** *ip_address***}**

[vrf *name***] ftp admin-state [enable | disable]**

Syntax Definitions

name	The name of the VRF.
default	Sets the port back to the default of 21.
service_port	The TCP service port number. Must be 21 or between between 20000-20999.
**enable	disable**	Enables or disables FTP access.
ip_address	Specifies the IPv4 address for the FTP session.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- You must have a valid username and password for the specified host.
- The default FTP directory is **/flash**.

Examples

```
-> ftp port 20000
-> ftp admin-state disable
-> ftp 172.17.6.228
-> vrf vrf1 ftp admin-state enable
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; **vrf** parameter added.

Related Commands

cd	Changes the current working directory of the switch.
pwd	Displays the current working directory of the switch.
ls	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
   alaIpFtpAdminStatus
```

show ftp

Displays the current FTP server settings like the port used for FTP, the FTP server's status in the given VRF.

[vrf *name***] show ftp**

Syntax Definitions

name	The name of the VRF.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show ftp
Ftp Admin-State = Enabled
Ftp Port = 21
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; **vrf** parameter added.

Related Commands

ftp	Starts an FTP session.

MIB Objects

```
alaIpFtpAdminStatus
alaIpFtpPort
```

63 Web Management Commands

The switch can be configured and monitored using WebView, which is a web-based device management tool. Web Management CLI commands allow you to enable/disable web-based management and configure certain WebView parameters, such as Secure Socket Layer (SSL).

MIB information for the Web Management commands is as follows:

Filename: ALCATEL-IND1-WEBMGT-MIB.mib
Module: alcatelIND1WebMgtMIB

A summary of the available commands is listed here:

webview server

Enables or disables the web management server on the switch.

[vrf *name***] webview server {enable | disable}**

Syntax Definitions

name	The name of the VRF.
enable	Enables the web management server on the switch.
disable	Disables the web management server on the switch.

Defaults

parameter	default
WebView Server	Enabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If the WebView Server is disabled, WebView Access is automatically disabled.
- VRF name must either be ‘default’or pre-defined VRF (user-defined).

Examples

```
-> webview server enable
-> webview server disable
-> vrf vrf1 webview server enable
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **vrf** parameter added.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtServerStatus
```

webview access

Enables or disables web management access on the switch.

[vrf *name***] webview access {enable | disable}**

Syntax Definitions

name	The name of the VRF.
enable	Enables the web management access on the switch.
disable	Disables the web management access on the switch.

Defaults

parameter	default
WebView Access	Enabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If Web Access is enabled, the WebView Server is automatically enabled.
- VRF name must either be ‘default’or pre-defined VRF (user-defined).

Examples

```
-> webview access enable
-> webview access disable
-> vrf vrf1 webview access enable
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **vrf** parameter added.

Related Commands

webview server	Enables/disables the web server on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtAdminStatus
```

webview force-ssl

Enables or Disables Force SSL on the switch. SSL is a protocol that establishes and maintains secure communication between SSL-enabled servers and clients.

webview force-ssl {enable | disable}

Syntax Definitions

enable	Enables the requirement to use SSL to access the switch when using WebView.
disable	Disables the requirement to use SSL to access the switch when using WebView.

Defaults

parameter	default
Force SSL	Enabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

The switch contains a self-signed certificate that may prompt a certificate warning.

Examples

```
-> webview force-ssl enable
-> webview force-ssl disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtSsl
```

webview http-port

Changes the port number for the embedded web management server.

webview http-port {default | port *port***}**

Syntax Definitions

default	Restores the port to its default (80) value.
port	The desired port number for the embedded Web server. The number must be in the range 0 to 65535; well-known port numbers cannot be configured.

Defaults

parameter	default
port	80

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

All WebView sessions must be terminated before entering this command.

Examples

```
-> webview http-port port 1025
-> webview http-port default
```

Release History

Release 7.1.1; command was introduced.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaIND1WebMgtHttpPort
```

webview https-port

Changes the default secure (HTTPS) port for the embedded web management server.

webview https-port {default | port *port***}**

Syntax Definitions

default	Restores the port to its default (443) value.
port	The desired HTTPS port number. The number must be in the range 0 to 65535; well-known port numbers cannot be configured.

Defaults

parameter	default
port	443

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

All WebView sessions must be terminated before entering this command.

Examples

```
-> webview https-port port 1026
-> webview https https-port default
```

Release History

Release 7.1.1; command was introduced.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaIND1WebMgtHttpsPort
```

webview ssl-strong-ciphers

Enables or disables support of only SSL strong cipher algorithms in order to prevent client opening connections to the switch using weak algorithms.

webview ssl-strong-ciphers {enable | disable}

Syntax Definitions

enable	Enables the strong cipher requirement.
disable	Disables the strong cipher requirement.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

When enabled the following algorithms will not be supported: RC4-SHA, RC4-MD5, ECDHE-RSA-RC4-SHA, IDEA-CBC-SHA, DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, ECDHE-RSA-DES-CBC3-SHA, aNULL, eNULL, EXPORT, DES, MD5, PSK, RC4.

Examples

```
-> webview ssl-strong-ciphers enable
-> webview ssl-strong-ciphers disable
```

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaIND1WebMgtSSLStrongCiphers
```

webview wlan cluster-virtual-ip precedence

Sets the preference for obtaining the cluster virtual IP address for WebView re-direct. The WLAN cluster virtual IP address can be obtained from LLDP or configured manually. The precedence allows to set the preference between the LLDP and manual configuration in case when both are available.

webview wlan cluster-virtual-ip precedence {lldp | configured}

Syntax Definitions

lldp	The preference to obtain the WLAN cluster virtual IP address is set to LLDP.
configured	The preference to obtain the WLAN cluster virtual IP address is set to the manually configured WLAN cluster virtual IP address.

Defaults

parameter	default
lldp | configured	lldp

Platforms Supported

OmniSwitch 6860, 6865, 9900

Usage Guidelines

- Use this command to set the preference for obtaining the cluster virtual IP address for WebView re-direct.
- If more than one cluster virtual IP address is obtained through LLDP on the same port, the recently obtained IP is considered.
- If more than one cluster virtual IP is obtained through LLDP on different ports, the recently obtained IP is considered.
- If the precedence is set for LLDP obtained IP address, but there is no LLDP obtained cluster virtual IP address, then the manually configured cluster virtual IP address will be considered if configured.
- If the precedence is set for manually configured cluster virtual IP address, but there is no configured IP address present, then the LLDP obtained cluster virtual IP address will be considered if received.

Examples

```
-> webview wlan cluster-virtual-ip precedence lldp
-> webview wlan cluster-virtual-ip precedence configured
```

Release History

Release 8.4.1 R02; command was introduced.

Related Commands

show webview wlan config	Displays the AP cluster virtual IP configured on the switch.

MIB Objects

```
alaIND1WebMgtWlanIpPrecedence
```

webview wlan cluster-virtual-ip

Configures the cluster virtual IP address of the Access Point (AP) in the switch. The WebView server on the switch redirects the URL to the AP (Virtual IP Address) URL when the WLAN Management is accessed from WebView.

webview wlan cluster-virtual-ip *virtual-ip-address-of-wlan-cluster*

Syntax Definitions

virtual-ip-address-of-wlan-cluster	Virtual IP address (IPV4) of the AP cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 9900

Usage Guidelines

Use this command to configure the AP cluster virtual IP address to access the OAW-AP web interface from the webview.

Examples

```
-> webview wlan cluster-virtual-ip 10.25.6.8
```

Release History

Release 8.4.1 R02; command was introduced.

Related Commands

show webview wlan config	Displays the AP cluster virtual IP configured on the switch.

MIB Objects

```
alaIND1WebMgtWlanConfiguredIpAddress
```

show webview wlan config

Displays the cluster virtual IP precedence configuration, WLAN AP cluster virtual IP configured on the switch, and WLAN AP cluster virtual IP obtained through LLDP.

show webview wlan config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6865, 9900

Usage Guidelines

N/A

Examples

```
-> show webview wlan config
WebView WLAN Cluster-Virtual-IP Precedence = LLDP
WebView WLAN Cluster-Virtual-IP configured address = 0.0.0.0
WebView WLAN Cluster-Virtual-IP LLDP address = 1.1.1.1
```

output definitions

WebView WLAN Cluster-Virtual-IP Precedence	The precedence set for obtaining the cluster virtual IP address of the AP.
WebView WLAN Cluster-Virtual-IP configured address	The manually configured cluster virtual IP address.
WebView WLAN Cluster-Virtual-IP LLDP address	The cluster virtual IP address obtained from the LLDP packets.

Release History

Release 8.4.1R02; command was introduced.

Related Commands

webview wlan cluster-virtual-ip precedence	Allows to set the preference for the choice of cluster virtual IP address for WebView re-direct.
webview wlan cluster-virtual-ip	Configures the virtual IP address of the Access Point (AP) clusters in the switch.

MIB Objects

```
alaIND1WebMgtWlanIpPrecedence
   alaIND1WebMgtWlanConfiguredIpAddressType
   alaIND1WebMgtWlanConfiguredIpAddress
   alaIND1WebMgtWlanLldpIpAddressType
   alaIND1WebMgtWlanLldpIpAddress
```

show webview

Displays web management configuration information.

[vrf *name***] show webview**

Syntax Definitions

name	The name of the VRF.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

If a VRF name is specified, the enabled/disabled state for WebView Server and WebView Access for the specified VRF is displayed.

Examples

```
-> show webview

WebView Server = Enabled
WebView Access = Enabled
WebView Force-SSL = Enabled
WebView HTTPS-Port = 443
WebView SSL-Strong-Ciphers = Enabled

vrf1::-> show webview
WebView Server = Enabled,
WebView Access = Enabled,
WebView Force-SSL = Enabled,
WebView HTTPS-Port = 443
WebView SSL-Strong-Ciphers = Enabled
```

output definitions

WebView Server	Indicates whether web management server is enabled or disabled.
WebView Access	Indicates whether web management access is enabled or disabled.
Force SSL	Indicates whether Force SSL is enabled or disabled. If this is enables it means that SSL is forced on an HTTP session and hence HTTPS protocol is negotiated between the client and server.
Web Management Https Port	The port configured for a secure HTTP connection (SSL enabled).
Web SSL-Strong-Ciphers	Indicates whether SSL strong cipher requirement is enabled or disabled.

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **vrf** parameter added.

Related Commands

webview server	Enables/disables web management server on the switch.
webview access	Enables/disables webview access on the switch.
webview force-ssl	Enables/disables SSL on the switch.
webview ssl-strong-ciphers	Enables/disables SSL strong ciphers on the switch.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
   alaInd1WebMgtServerStatus
   alaInd1WebMgtAdminStatus
   alaInd1WebMgtSsl
   alaInd1WebMgtHttpsPort
   alaInd1WebMgtSSLStrongCiphers
```

64 Configuration File Manager Commands

The Configuration Manager feature allows you to configure your switch using an ASCII-based text file. CLI commands may be typed into a text document—referred to as a *configuration file*—and then uploaded and applied to the switch.

MIB information for the Configuration Manager commands is as follows:

Filename: ALCATEL-IND1-CONFIG-MGR-MIB.mib
Module: alcatelIND1ConfigMgrMIB

A summary of the available commands is listed here:

configuration apply

Applies a configuration file to the switch. Files may be applied immediately or after a designated timer session. With the timer session option, files are applied either at a scheduled date and time or after a specified period of time (i.e., a countdown) has passed.

configuration apply *filename* **[at** *hh:mm month dd* **[***year***]] | [in** *hh***[***:mm***]] [verbose]**

Syntax Definitions

filename	The name of the configuration text file to be applied to the switch (e.g., **newfile1**).
at *hh:mm* **{***dd month* | *month dd***} [***year***]**	Designates a timer session in which a configuration file is applied at a specified date and time in the future. Values for *hh* range from 00 through 23. Values for *mm* range from 00 through 59. Values for *dd* range from 01 through 31. Values for month range from january through december. The switch assumes either the current year or the next calendar year for month and day pairs that precede the current date.
in *hh***[***:mm***]**	Designates a timer session in which the configuration file is applied after a specific amount of time (i.e., a countdown) has passed. Values for *hh* range from 00 through 23. Values for *mm* range from 00 through 59.
verbose	When verbose is entered, information is displayed on your workstation's console as each command in the configuration file is applied.

Defaults

By default, **verbose** error checking is not performed.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The **configuration apply** command only applies settings to the running configuration. The **boot.cfg** file does not get overwritten.
- It is recommended that you check all configuration files for syntax errors before applying them to your switch.
- To schedule a timer session in which a file is applied at a specific date and time, enter **at** followed by the hour, minute, month, day, and year. The switch assumes either the current calendar year or the next calendar year for dates beginning January 1.
- To schedule a timer session in which a file is applied after a specific amount of time (i.e., a countdown) has passed, enter **in** followed by the number of hours and minutes.
- Verbose mode is not supported for timer sessions.
- The keyword, **authkey**, along with a related alpha-numeric text string, are automatically included in many snapshot files (e.g., **configuration snapshot all**). The text string following the **authkey** keyword

represents a login password that has been encrypted *twice*. (The first encryption occurs when a password is first created by a user; the second encryption occurs when a configuration snapshot is taken.) This dual encryption further enhances switch security. However, it is important to note that any configuration file (including a generated snapshot) that includes this dual-encrypted password information will result in an error whenever it is applied to the switch via the **configuration apply** command. This is a valid switch function and does not represent a significant problem. If an **authkey**-related error is the *only* error detected, simply remove all **authkey**-related syntax using a text editor. If a new password is required for the switch, include valid password syntax in the configuration file or immediately issue a new password by using the **password** command at the command prompt. For more information on passwords, refer to page 38-60.

Examples

```
-> configuration apply new_configuration at 12:00 15 november
-> configuration apply new_configuration at 12:00 november 15
-> configuration apply newfile1 in 01:30
-> configuration apply my_switch_config in 00:05
-> configuration apply asc.1.snap in 23:00
-> configuration apply aaa_config in 12
-> configuration apply vlan_config verbose
-> configuration apply vlan_config
...
```

Note. When the **configuration apply** command is entered *without* **at** or **in** syntax information, one or more dots "**.**" is displayed in the next line, immediately following the command line. This indicates command progress; each dot represents 256 text lines in the configuration file processed by the configuration apply mechanism.

Release History

Release 7.1.1; command was introduced.

Related Commands

configuration syntax-check	Performs a syntax and authorization check of all CLI commands contained in a configuration file.

MIB Objects

```
alcatelIND1ConfigMgrMIBObjects
   configFileName
   configFileMode
   configFileAction
   configTimerFileName
   configTimerFileTime
```

configuration error-file-limit

Specifies the maximum number of configuration error files allowed in the switch's **/flash** directory. Error files are normally generated when a configuration file is applied to the switch. Error files are identified by their **.err** extension.When the maximum number of **.err** files is exceeded, any new error file will overwrite the **.err** file with the oldest timestamp.

configuration error-file-limit *number*

Syntax Definitions

number	Indicate the number of error files allowed in the **/flash** directory. The valid range is from 1 to 25 files.

Defaults

parameter	default
number	1

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When the error file limit is set to 1 (the default value), the next error file generated by the switch will replace the existing one.
- When the error file limit is set to a value greater than 1, when a new error file that exceeds the maximum limit is created, the switch will automatically remove the error file with the smallest timestamp.
- The error files generated by the switch have the **.err** extension.
- If you want to save an error file, you may change the file name so that it does not have the **.err** extension, or you can move it from the /flash directory.

Examples

```
-> configuration error-file-limit 2
-> configuration error-file-limit 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
configuration cancel	Cancels a pending timer session for a configuration file.

MIB Objects

```
alcatelIND1ConfigMgrMIBObjects
   configErrorFileMaximum
```

show configuration status

Displays whether there is a pending timer session scheduled for a configuration file and indicates whether the running configuration and the saved configuration files are *identical* or *different*. This command also displays the number of error files that will be held in the flash directory.

show configuration status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- A timer session can be scheduled using the **configuration apply** command. For more information, refer to page 64-2.
- The screen output **File configuration** <*/path/filename*>**: scheduled at** *dd/mm hh:mm* indicates that a timer session has been scheduled for a later time.
- The output **No file configuration has been scheduled** indicates an idle timer session (i.e., no timer session has been scheduled for a configuration file).
- The output **File configuration is in progress** indicates that a file is currently being applied to the switch.
- The output **File configuration** <*/path/filename*>**: completed with 2 errors** indicates that the named file was applied to the switch with two recorded errors.
- When the running and saved configurations are the same, the output **Running configuration and saved configuration are identical** will be displayed.
- When the running and saved configurations are the different, the output **Running configuration and saved configuration are different** will be displayed.
- To synchronize the running and saved configuration, use the **write memory** command.

Examples

```
-> show configuration status
```

Release History

Release 7.1.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
configuration cancel	Cancels a pending timer session for a configuration file.
configuration error-file-limit	Specifies the maximum number of configuration error files allowed in the switch's **/flash** directory.
write memory	Copies the running configuration (RAM) to the working directory.

MIB Objects

```
configTimerFileGroup
   configTimerFileStatus
```

configuration cancel

Cancels a pending timer session for a configuration file.

configuration cancel

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> configuration cancel
```

Release History

Release 7.1.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
show configuration status	Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

```
configTimerFileGroup
   configTimerClear
```

configuration syntax-check

Performs a syntax and authorization check of all CLI commands contained in a configuration file.

configuration syntax-check *path/filename* **[verbose]**

Syntax Definitions

path/filename	The configuration file being checked for syntax and authorization errors. If a configuration file is located in another directory, be sure to specify the full path. For example, **/flash/working/asc.1.snap**.
verbose	When **verbose** is specified in the command line, all syntax contained in the configuration file is printed to the console, even if no error is detected. When **verbose** is *not* specified in the command line, cursory information (number of errors and error log file name) will be printed to the console *only if a syntax or configuration error is detected*.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- When an error is detected, an error file (**.err**) is automatically generated by the switch. By default, this file is placed in the root **/flash** directory. To view the contents of a generated error file, use the **view** command. For example, **view asc.1.snap.1.err**.
- The syntax, **mac alloc**, is automatically included in many snapshot files (e.g., **configuration snapshot all**). All **mac alloc**-related syntax is valid *during switch boot up only* (i.e., it cannot be applied while the switch is in run-time operation). Because snapshot files are commonly used as configuration files, syntax checks may detect **mac alloc** syntax and issue an error (along with a generated **.err** file). This is a valid switch function and does not represent a significant problem. If a **mac alloc**-related error is the *only* error detected, simply remove the syntax using a text editor, then re-check the file using the **configuration syntax-check** command.
- It is recommended that you check all configuration files for syntax errors before applying them to your switch.

Examples

```
-> configuration syntax-check vlan_file1
..
```

Note. When the **configuration syntax-check** command is entered, one or more dots "**.**" is displayed in the command output. This indicates command progress; each dot represents 256 text lines in the configuration file processed by the syntax check mechanism.

Release History

Release 7.1.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
show configuration status	Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

```
configFileGroup
   configErrorFileName
   configErrorFileMaximum
   configFileMode
   configFileStatus
```

configuration snapshot

Generates a snapshot file of the switch's non-default current running configuration. A snapshot can be generated for all current network features or for one or more specific network features. A snapshot is a single text file that can be viewed, edited, and reused as a configuration file.

configuration snapshot [*feature_list* **| all} [***path/filename***]**

Syntax Definitions

feature_list	The description for the network feature(s) to be included in the snapshot. You may enter more than one network feature in the command line. Enter a question mark (?) on the command line to get a list of features (**configuration snapshot ?**).
all	Includes all network features in the snapshot.
path/filename	A user-defined name for the resulting snapshot file. For example, **test_snmp_snap**. You may also enter a specific path for the resulting file. For example, the syntax **/flash/working/test_snmp_snap** places the **test_snmp_snap** file in the switch's **/flash/working** directory.

Defaults

If a file name is not specified, the default file name **asc.#.snap** is used. Here, # indicates the order in which the default file is generated. For example, the first default file name to be generated is **asc.1.snap**, the second default file name to be generated is named **asc.2.snap**, etc. By default, all snapshot files are placed in the root **/flash** directory.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Only current, non-default configuration settings are written to the snapshot file.
- You may enter more than one network feature in the command line. Separate each network feature with a space and no comma. Network features may be entered in any order.
- The snapshot file is automatically placed in the root **/flash** directory unless otherwise specified.

Examples

```
-> configuration snapshot all
-> configuration snapshot qos health aggregation new_file1
-> configuration snapshot snmp_snapshot snmp
-> configuration snapshot 802.1q

-> configuration snapshot ?
                          ^
                          ZEROCONF WEBMGT VRRP VM-SNOOPING VLAN VIRTUAL-CHASSIS
                          VFC VCSP UDLD SYSTEM SVCMGR STP SPB-ISIS SNMP SLB SIP
                          SESSION SECURITY SAA RIPNG RIP QOS QMR PVLAN PTP
                          PPPOE-IA PORT-MAPPING PORT-MANAGER POLICY PMM OSPF3
```

```
OSPF OPENFLOW NTP NETSEC MVRP MULTI-CHASSIS MODULE
MACSEC LOOPBACK-DETECTION LLDP LINKAGG
LINK-FAULT-PROPAGATION LDP LANPOWER ISIS IPV6 IPSEC
IPMS IPMR IP-ROUTING IP-HELPER IP INTERFACE HEALTH
HA-VLAN FCOE ETHERNET-OAM ERP EFM-OAM DHL
DHCPV6-SERVER DHCPV6-RELAY DHCP-SNOOPING DHCP-SERVER
DHCP-MESSAGE-SERVICE DHCP-ACTIVE-LEASE-SERVICE
DEVICE-PROFILE DA-UNP CLOUD-AGENT CHASSIS CAPABILITY
BRIDGE BGP BFD AUTO-FABRIC APP-MONITORING
APP-FINGERPRINT ALL ALARM-MANAGER AAA
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show configuration snapshot Displays the switch's current running configuration.

MIB Objects

```
configManager
   configSnapshotFileName
   configSnapshotAction
   configSnapshotAllSelect
```

show configuration snapshot

Displays the switch's current running configuration for all features or for the specified feature(s).

show configuration snapshot [*feature_list***]**

Syntax Definitions

feature_list	Specify the feature(s) for which you want to display the running configuration. List the features separated by a space with no comma. Enter a question mark (?) on the command line to get a list of features (**show configuration snapshot ?**).

Defaults

By default, this command shows configuration information for *all* features.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use this command to view the current configuration for any feature shown in the table.
- Configurations are listed below the name of each feature.
- Features with no current configuration show only the name of the feature.

Examples

```
-> show configuration snapshot
-> show configuration snapshot aaa bridge
! Bridging :

! AAA :
aaa authentication default "local"
aaa authentication console "local"
user "public" read All write All no auth authkey 391b0e74dbd13973d703cceaa4a8e30

-> show configuration snapshot ?
                                        ^
                                        <cr> ZEROCONF WEBMGT VRRP VM-SNOOPING
                                        VLAN VIRTUAL-CHASSIS VFC VCSP UDLD
                                        SYSTEM SVCMGR STP SPB-ISIS SNMP SLB
                                        SIP SESSION SECURITY SAA RIPNG RIP QOS
                                        QMR PVLAN PPPOE-IA PORT-MAPPING
                                        PORT-MANAGER POLICY PMM OSPF3 OSPF
                                        OPENFLOW NTP NETSEC MVRP MULTI-CHASSIS
                                        MODULE MACSEC LOOPBACK-DETECTION LLDP
                                        LINKAGG LINK-FAULT-PROPAGATION LDP
                                        LANPOWER ISIS IPV6 IPSEC IPMS IPMR
                                        IP-ROUTING IP-HELPER IP INTERFACE
                                        HEALTH HA-VLAN FCOE ETHERNET-OAM
                                        ERP EFM-OAM DHL DHCPV6-SERVER
```

```
DHCPV6-RELAY DHCP-SNOOPING DHCP-SERVER
DHCP-MESSAGE-SERVICE
DHCP-ACTIVE-LEASE-SERVICE
DEVICE-PROFILE DA-UNP CLOUD-AGENT
CHASSIS CAPABILITY BRIDGE BGP BFD
AUTO-FABRIC APP-MONITORING
APP-FINGERPRINT ALL ALARM-MANAGER AAA
```

Release History

Release 7.1.1; command was introduced.

Related Commands

write terminal	Displays the switch's current running configuration for all features.

MIB Objects

```
configManager
   configSnapshotFileName
   configSnapshotAction
   configSnapshotAllSelect
```

write terminal

Displays the switch's current running configuration for all features.

write terminal

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Configurations are listed below the name of each feature.
- Features with no current configuration show only the name of the feature.

Examples

```
-> write terminal
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show configuration snapshot	Displays the switch's current running configuration for all features or for the specified feature(s).

MIB Objects

```
configManager
   mib_configSnapshotAllSelect
```

configuration apply network-sync

Performs pre-provisioning or runtime network level synchronization for AOS Micro Services (AMS) using the publisher/subscriber model.

configuration apply network-sync *filename* **[community** *community-name* **| local-apply]**

Syntax Definitions

filename	The name of the file with the AOS configuration to be synchronized.
community-name	Performs synchronization only on switches with the corresponding community name.
local-apply	Apply the configuration to the local switch.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Use the **configuration syntax-check** command to validate the configuration file syntax before network synchronization.
- It is recommended to have only global, and not local, level switch configuration information propagated for network level configurations.
- The file name “preprovision.txt” is a pre-defined name used for pre-provisioning purposes. Pre-provisioning applies only to new nodes that join the network, the configuration will not be applied to existing nodes. Refer to the AMS section of the Switch Management Guide for additional information.

Examples

```
-> configuration apply network-sync preprovision.txt
-> configuration apply network-sync adaptive-test
```

Release History

Release 8.6R1; command not supported.

Related Commands

configuration syntax-check	Performs a syntax and authorization check of all CLI commands contained in a configuration file.

MIB Objects

N/A

65 SNMP Commands

This chapter includes descriptions for Trap Manager and SNMP Agent commands. The commands are used for configuring SNMP settings on the switch.

- SNMP station commands can create, modify, or delete an SNMP station. Also included is a show command for monitoring current SNMP station status.
- SNMP trap commands configure SNMP trap settings. Traps can be replayed and filtered. Also, test traps can be generated to verify that individual traps are being correctly handled by the Network Management Station (NMS). The SNMP trap commands set includes show commands for monitoring SNMP trap information.
- SNMP agent commands configure SNMP security levels on the switch. Also includes show commands for monitoring the current SNMP security status.

MIB information for SNMP Community commands is as follows:

Filename: SNMP-COMMUNITY-MIB.mib
Module: snmpCommunityMIB

MIB information for Trap Manager commands is a follows:

Filename ALCATEL-IND1-TRAP-MGR-MIB.mib
Module: alcatelIND1TrapMgrMIB

MIB information for SNMP Agent commands is a follows:

Filename: ALCATEL-IND1-SNMP-AGENT-MIB.mib
Module: alcatelIND1SNMPAgentMIB

A summary of the available commands is listed here:

SNMP station commands	**snmp station** **show snmp station**
SNMP engine ID commands	**snmp snmp-engineid-type** **show snmp snmp-engineid**
SNMP community map commands	**snmp community-map** **snmp community-map mode** **show snmp community-map**
SNMP security commands	**snmp security** **snmp security tsm** **snmp tsm-map** **show snmp tsm-map** **show snmp security** **show snmp statistics** **show snmp mib-family**
SNMP trap commands	**snmp-trap absorption** **snmp-trap to-webview** **snmp-trap replay-ip** **snmp-trap filter-ip** **snmp authentication-trap** **show snmp-trap replay-ip** **show snmp-trap filter-ip** **show snmp authentication-trap** **show snmp-trap config**
Event commands	**event-action** **show event-action**

snmp station

Adds a new SNMP station; modifies or deletes an existing SNMP station.

snmp station {*ip_address* **|** *ipv6_address* **|** *domain_name***} {[***port***] [***username***] [v1 | v2 | v3 | v3 tsm local-identity** *local_string* **remote-identity** *remote_string*] **[enable | disable]}**

no snmp station {*ip_address* **|** *ipv6_address* **|** *domain_name***}**

Syntax Definitions

ip_address	The IP address to which SNMP unicast traps will be sent.
ipv6_address	The IPv6 address to which SNMP unicast traps will be sent.
domain_name	A Fully Qualified Domain Name (FQDN) to which SNMP unicast traps will be sent. Specify a domain name up to 255 characters in length.
port	A UDP or TLSTCP destination port.
username	The user name on the switch or external server used to send traps to the SNMP station(s). The username specified here must match an existing user account name.
v1	Specifies that traps are sent using SNMP version 1.
v2	Specifies that traps are sent using SNMP version 2.
v3	Specifies that traps are sent using SNMP version 3.
tsm	The TSM security model for SNMP. The security model can be selected only for SNMP version 3.
local_string	The file name of the local certificate. To be configured when TSM mode is selected.
remote_string	The file name of the remote certificate. To be configured when TSM mode is selected.
enable	Enables the specified SNMP station.
disable	Disables the specified SNMP station.

Defaults

parameter	default
port	162 (for UDP) 10162 (for TLSTCP)
v1 | v2 | v3	**v3**
enable | disable	**enable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of the command to remove an existing SNMP station.
- When adding an SNMP station, specify an IP address or FQDN *plus username parameters*. For example, the syntax **snmp station 1.2.3.4** is not a valid command entry; however, **snmp station 1.2.3.4 username1** is a valid command entry.
- A maximum of 50 SNMP sessions can be established in the switch.
- When modifying an SNMP station, specify an IP address or FQDN *plus at least one additional parameter*. For example, the syntax **snmp station 1.2.3.4** is not a valid command entry; however, **snmp station 1.2.3.4 v2** is a valid command entry.
- When an FQDN is specified with this command, the switch will resolve the domain name to an IP address. Make sure the domain name maps to a valid and reachable IP address.
- When the SNMP station is enabled, the switch transmits traps to the specified IP or IPv6 address.
- For UDP the default port 162 is commonly used for traps; however, the destination port can be redefined to accommodate an SNMP station using a nonstandard port. The destination port specified must correspond with the UDP destination port configured at the receiving SNMP station(s).
- For TLSTCP the default port 10162 is commonly used for traps; however, the destination port can be redefined to accommodate an SNMP station using a nonstandard port. The destination port specified must correspond with the TLSTCP destination port configured at the receiving SNMP station(s).
- To send SNMP traps over TLS connection, the SNMP station needs to be configured with TSM user along with certificate identities.
- The local_identity and remote_identity are the names of certificate file. If the contents of local or remote certificates are changed, the updated certificates must be manually copied from master or primary to all secondaries and slaves. A reboot is required for the changes to be applied.
- When TSM security model is enabled, all the v1/v2/v3 USM requests and traps are discarded.
- When TSM security model is disabled, all v1/v2/v3 (USM and TSM) requests and traps are allowed.
- In TSM security model SNMP requests are supported over IPv4 transport only.

Examples

```
-> snmp station 168.22.2.2 111 username2 v1 disable
-> snmp station 168.151.2.101 "test lab"
-> snmp station 170.1.2.3 username1 enable
-> snmp station 1.1.2.2 v2
-> no snmp station 2.2.2.2
-> snmp station 300::1 enable
-> no snmp station 300::1

-> snmp station upam.omnivista.com username2 v1 disable
-> snmp station upam.omnivista.com v2
-> no snmp station upam.omnivista.com
-> snmp station opendaylight.com enable v2 public
ERROR: DNS lookup failed, unknown host opendaylight.com
-> snmp station 168.22.1.1 joe v3 tsm local-identity aluSubagent.crt
remote-identity manager.crt enable
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R1; *domain_name* parameter option added.
Release 8.6R1; **tsm**, **local-identity**, and **remote-identity** parameters added**.**

Related Commands

show snmp station	Displays the current SNMP station information.

MIB Objects

```
trapStationTable
   trapStationIP
   trapStationPort
   trapStationUser
   trapStationProtocol
   trapStationRowStatus
alaTrapInetStationTable
   alaTrapInetStationIPType
   alaTrapInetStationIP
   alaTrapInetStationPort
   alaTrapInetStationRowStatus
   alaTrapInetStationProtocol
   alaTrapInetStationUser
   alaTrapInetStationSecurityModel
   alaTrapInetStationLocalIdentity
   alaTrapInetStationRemoteIdentity
```

show snmp station

Displays the current SNMP station status and details.

show snmp station [details]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show snmp station
ipAddress/Port           status    protocol user
--------------------------------------------------------------------------------
199.199.100.200/8010        enable    v3       NMSuserV3MD5DES
199.199.101.201/111         disable   v2       NMSuserV3MD5
199.199.102.202/8002        enable    v1       NMSuserV3SHADES
199.199.103.203/8003        enable    v3       NMSuserV3SHADES
199.199.104.204/8004        enable    v3       NMSuserV3SHA

-> show snmp station details
ipAddress/port:    10.255.24.59/162,
  status:          disable,
  protocol:        v2,
  user:            public,

ipAddress/port:    135.115.207.36/162,
  status:          disable,
  protocol:        v2,
  user:            public,

ipAddress/port:    localhost/10162,
  status:          disable,
  protocol:        v3,
  security model:  tsm,
  user:            joecool,
  local identity:  aluSubagent.crt,
  remote identity: manager.crt,

ipAddress/port:    10.255.24.57/162,
  status:          enable,
  protocol:        v1,
```

```
user:           public,
```

output definitions

IpAddress	IP Address of the SNMP management station.
Port	Trap station port number (UDP, TLSTCP).
status	The Enabled/Disabled status of the SNMP management station.
protocol	The version of SNMP set for this management station.
security model	Displays the security model selected.
user	The user account name.
local identity	File name of local certificate used, TSM only. This is displayed only for SNMP version 3.
remote identity	File name of remote certificate used, TSM only. This is displayed only for SNMP version 3.

Release History

Release 7.1.1; command was introduced.
Release 8.6R1; **details** parameter and **local identity**, **remote identity**, and **security model** output fields added.

Related Commands

snmp station	Adds a new SNMP station; modifies or deletes an existing SNMP station.

MIB Objects

```
trapStationTable
   trapStationIP
   trapStationPort
   trapStationUser
   trapStationProtocol
   trapStationRowStatus
alaTrapInetStationTable
   alaTrapInetStationIPType
   alaTrapInetStationIP
   alaTrapInetStationPort
   alaTrapInetStationRowStatus
   alaTrapInetStationProtocol
   alaTrapInetStationUser
   alaTrapInetStationLocalIdentity
   alaTrapInetStationRemoteIdentity
```

snmp snmp-engineid-type

Configures a unique engine ID for the OmniSwitch SNMP agent.

snmp snmp-engineid-type {text | mac-address | ipv4-address | ipv6-address} snmp-engineid {*text_string* **|** *mac_address* **|** *ipv4_address* **|** *ipv6_address***}**

snmp snmp-engineid-type mac-address snmp-engineid default

Syntax Definitions

text_string	A text string that will be converted to a hexadecimal value. The valid range is 1–27 characters.
mac_address	A specific MAC Address (for example, 00:00:39:59:f1:0c).
ipv4_address	An IPv4 address that will be converted to a hexadecimal value.
ipv6_address	An IPv6 address that will be converted to a hexadecimal value.

Defaults

By default, the SNMP engine ID is set to the base MAC address for the switch appended to the enterprise value for OmniSwitch platforms (for example, if the enterprise value is “8000195603” and the switch base MAC address is “2c:fa:a2:13:e4:02”, then the default engine ID is set to “80001956032cfaa213e402”).

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To set the engine ID back to the default value, specify the **mac-address** parameter and the **default** parameter with this command. For example, **snmp snmp-engineid-type mac-address snmp-engineid default**.
- Note that the **snmp-engineid** keyword is entered after the parameter that specifies the type of engine ID format to use and before the actual value that matches the specified parameter type. For example, if the **ipv4-address** parameter is specified, enter the IPv4 address value after the **snmp-engineid** keyword (**snmp snmp-engineid-type ipv4-address snmp-engineid 10.2.2.1**).
- When a text string, an IPv4 address, or an IPv6 address is specified, the value is automatically converted to a hexadecimal value that is then appended to the OmniSwitch enterprise value to form the SNMP engine ID for the switch.

Examples

```
-> snmp snmp-engineid-type text snmp-engineid "test lab"
-> snmp snmp-engineid-type mac-address snmp-engineid 00:2a:95:01:02:03
-> snmp snmp-engineid-type ipv4-address snmp-engineid 168.22.2.2 111
-> snmp snmp-engineid-type mac-address snmp-engineid default
```

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show snmp snmp-engineid	Displays the current SNMP engine ID information.

MIB Objects

```
snmpAgtEngineIdType
snmpAgtEngineId
```

show snmp snmp-engineid

Displays the current SNMP engine ID value for the switch.

show snmp snmp-engineid

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guideline

N/A

Examples

```
-> show snmp snmp-engineid
snmp engineId type         snmp engineId
------------------+------------------------------
   default Mac               80001956032cfaa213e402
```

output definitions

snmp engineId type	The type of engine ID (**default Mac**, **Text**, **Ipv4**, or **Ipv6**).
snmp engineId	The SNMP engine ID value that uniquely identifies the OmniSwitch SNMP agent. This value is comprised of the OmniSwitch enterprise ID plus the configured SNMP engine ID value, in hexadecimal format.

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

snmp snmp-engineid-type	Configures the type and value of the SNMP engine ID for the switch.

MIB Objects

```
snmpAgtEngineIdType
snmpAgtEngineId
```

snmp community-map

Configures and enables a community string on the switch and maps it to an existing user account name.

snmp community-map {[hash-key *string* **|** *community_string*] **user** *useraccount_name***} [enable | disable]**

no snmp community-map *community_string*

Syntax Definitions

hash-key *string*	The hashed format of a community string.
community_string	A community string in the form of a text string. This string must be between 1 and 32 characters.
useraccount_name	A user name in the form of a text string. This name must match a user login account name already configured on the switch or configured remotely on an external AAA server. This user name must be between 1 and 32 characters.
enable	Enables SNMP community string mapping.
disable	Disables SNMP community string mapping.

Defaults

By default, SNMP community map authentication is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Community strings are stored in a hashed format in the '**show configuration snapshot snmp**' output. To view community string mappings in plain-text use the **show snmp community-map** command.
- Community strings configured on the switch are used for v1 and v2c SNMP managers only.
- The user account name must be a current user account recognized by the switch. For a list of current user names use the **show user** command. To create a new user account, use the **user** command.
- There is one to one mapping between each community string and a user account name.
- Privileges attached to the community string are the ones inherited from the user account name that created it.
- The community-map mode must be enabled and the community string carried over each incoming v1 or v2c SNMP request must be mapped to a user account name in order to be processed by the SNMP agent.

Examples

```
-> snmp community-map community1 user testname1
-> snmp community-map community1 enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

snmp community-map mode Enables the local community strings database.

MIB Objects

```
SNMPCommunityTable
   snmpCommunityIndex
   snmpCommunitySecurityName
   snmpCommunityStatus
```

snmp community-map mode

Enables the local community strings database.

snmp community-map mode {enable | disable}

Syntax Definitions

enable	Enables SNMP community map database.
disable	Disables SNMP community map database.

Defaults

parameter	default
Community mode	disabled

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The community-map mode must be enabled and the community string carried over each incoming v1 or v2c SNMP request must be mapped to a user account name with SNMP privileges in order to be processed by the SNMP agent.
- When enabled, mapping is contained in the local community strings database populated by using the **snmp community-map** command.

Examples

```
-> snmp community-map mode enable
-> snmp community-map mode disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

snmp community-map	Configures and enables a community string on the switch and maps it to an existing user account name.

MIB Objects

```
SNMPCommunityTable
   snmpCommunityIndex
   snmpCommunitySecurityName
   snmpCommunityStatus
```

show snmp community-map

Shows the local community strings database.

show snmp community-map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guideline

N/A

Examples

```
-> show snmp community-map
Community mode : enabled

status   community string                 user name
--------+--------------------------------+--------------------------------
enabled   test_string1                   bb_usename
enabled   test_string2                   rr_usename
disabled  test_string3                   cc_usename
disabled  test_string4                   jj_usename
```

output definitions

Status	The Enabled/Disabled status of the community string.
Community String	The text that defines the community string.
User Name	The user account name.

Release History

Release 7.1.1; command was introduced.

Related Commands

snmp community-map	Configures and enables a community string on the switch and maps it to an existing user account name.

MIB Objects

N/A

snmp security

Configures SNMP security settings.

snmp security {no-security | authentication set | authentication all | privacy set | privacy all | trap-only | tls {enable | disable}}

Syntax Definitions

no-security	The switch will accept all SNMP v1, v2, and v3 requests.
authentication set	The switch will accept all requests *except* v1, v2, and non-authenticated v3 set requests. SNMP v1, v2, and non-authenticated v3 set requests will be rejected.
authentication all	The switch will accept all requests *except* v1, v2, and non-authenticated v3 get, get-next, and set requests. SNMP v1, v2, and non-authenticated v3 get, get-next, and set requests will be rejected.
privacy set	The switch will accept *only* authenticated SNMP v3 get, get-next and encrypted v3 set requests. All other requests will be rejected.
privacy all	The switch will accept only encrypted v3 get, get-next, and set requests. All other requests will be rejected.
trap-only	All SNMP get, get-next, and set requests will be rejected.
tls enable | disable	Unblocks (enable) or blocks (disable) the SNMP TLS port 10161.

Defaults

parameter	default
security	**privacy all**
tls enable | disable	**disable**

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Refer to the table below for a quick-reference list of security parameter and the SNMP request allowances for each parameter.

	v1 set v2 set v3 non-auth set	**v1 get v2 get v3 non-auth get/ get-next**	**v3 auth set**	**v3 auth get/ get-next**	**v3 encryp set**	**v3 encryp get/ get-next**
no-security	accepted	accepted	accepted	accepted	accepted	accepted
authentication set	rejected	accepted	accepted	accepted	accepted	accepted
authentication all	rejected	rejected	accepted	accepted	accepted	accepted
privacy set	rejected	rejected	rejected	accepted	accepted	accepted

	v1 set v2 set v3 non-auth set	**v1 get v2 get v3 non-auth get/ get-next**	**v3 auth set**	**v3 auth get/ get-next**	**v3 encryp set**	**v3 encryp get/ get-next**
privacy all	rejected	rejected	rejected	rejected	accepted	accepted
trap-only	rejected	rejected	rejected	rejected	rejected	rejected

Examples

```
-> snmp security no-security
-> snmp security authentication set
-> snmp security authentication all
-> snmp security privacy set
-> snmp security trap-only
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show snmp security	Displays the current SNMP security status.

MIB Objects

```
SNMPAgtConfig
   SnmpAgtSecurityLevel
```

snmp security tsm

Enables or disables TLS encryption for SNMP access.

snmp security tsm [enable | disable]

Syntax Definitions

enable	Enables TLS encryption for SNMP access.
disable	Disables TLS encryption for SNMP access.

Defaults

By default, the TLS encryption for SNMP access is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The TLS encryption can be enabled only for SNMP version 3.
- In Common Criteria mode (CC mode) TLS encryption for SNMP is enabled by default and cannot be disabled.

Examples

```
-> snmp security tsm enable
-> snmp security tsm disable
```

Release History

Release 8.6R1; command was introduced.

Related Commands

snmp tsm-map	Displays the current SNMP security status.

MIB Objects

```
SNMPAgtConfig
   snmpAgtTsmAdminState
```

snmp tsm-map

Allows to map a remote identity or certificate to a user in TSM mode.

snmp tsm-map remote-identity *remote_string* **user** *user_string*

Syntax Definitions

remote_string	File name of remote certificate to be mapped with the user. This string must be between 1 and 128 characters.
user_string	The user name. This string must be between 1 and 32 characters.

Defaults

N/A.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- The remote identity mapping for user can be done only in TSM mode.
- The remote identity mapping can be done for only one user at a time. It cannot be mapped to multiple users. Mapping it to a different user will replace the existing user.
- If the content of remote certificate is changed, the updated certificate must be manually copied from master or primary to all secondaries and slaves. A reboot is required for the changes to be applied.

Examples

```
-> snmp tsm-map remote-identity manager.crt user joe
-> snmp security tsm disable
```

Release History

Release 8.6R1; command was introduced.

Related Commands

show snmp tsm-map	Displays the current SNMP TSM remote identity mapping for a user.

MIB Objects

```
alaSnmpTsmUserTable
   alaSnmpTsmUserRemoteIdentity
   alaSnmpTsmUserName
```

show snmp tsm-map

Displays the current SNMP TSM remote identity mapping for a user.

show snmp tsm-map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

Enter the specific file name of the remote certificate to view the mapping related to it.

Examples

```
-> show snmp tsm-map
Remote Identity                    User
-----------------------------------+------------------------------
manager.crt                          adam

-> show snmp tsm-map manager.pem
Remote Identity                    User
-----------------------------------+------------------------------
manager.pem                        joecool
```

output definitions

Remote Identity	Displays the file name of the remote certificate mapped to the user.
User	Displays the user name mapped to the remote identity.

Release History

Release 8.6R1; command was introduced.

Related Commands

snmp tsm-map	Allows to map a remote identity or certificate to a user in TSM mode.

MIB Objects

N/A

show snmp security

Displays the current SNMP security status.

show snmp security [tsm]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Refer to the command on page 65-16 for descriptions of the five SNMP security states: no security, authentication set, authentication all, privacy set, privacy all, and trap only.
- Use the optional parameter **tsm** along with the command to display the configured SNMP TSM status.

Examples

```
-> show snmp security
snmp security = no security

-> show snmp security
snmp security = authentication set

-> show snmp security
snmp security = authentication all

-> show snmp security
snmp security = privacy set

-> show snmp security
snmp security = privacy all

-> show snmp security
snmp security = trap only

-> show snmp security tsm
snmp security tsm = disable
```

output definitions

snmp security	Displays the configured SNMP security level.
snmp security tsm	Displays the configured SNMP TLS encryption status.

Release History

Release 7.1.1; command was introduced.
Release 8.6R1; **tsm** parameter added.

Related Commands

snmp security	Configures the SNMP security settings.
snmp security tsm	Enables or disables TLS encryption for SNMP access.

MIB Objects

N/A

show snmp statistics

Displays the current SNMP statistics.

show snmp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show snmp statistics
From RFC1907
  snmpInPkts                    = 801
  snmpOutPkts                   = 800
  snmpInBadVersions             = 0
  snmpInBadCommunityNames       = 0
  snmpInBadCommunityUses        = 0
  snmpInASNParseErrs            = 0
  snmpEnableAuthenTraps         = disabled(2)
  snmpSilentDrops               = 0
  snmpProxyDrops                = 0
  snmpInTooBigs                 = 0
  snmpOutTooBigs                = 0
  snmpInNoSuchNames             = 0
  snmpOutNoSuchNames            = 0
  snmpInBadValues               = 0
  snmpOutBadValues              = 0
  snmpInReadOnlys               = 0
  snmpOutReadOnlys              = 0
  snmpInGenErrs                 = 0
  snmpOutGenErrs                = 0
  snmpInTotalReqVars            = 839
  snmpInTotalSetVars            = 7
  snmpInGetRequests             = 3
  snmpOutGetRequests            = 0
  snmpInGetNexts                = 787
  snmpOutGetNexts               = 0
  snmpInSetRequests             = 7
  snmpOutSetRequests            = 0
  snmpInGetResponses            = 0
  snmpOutGetResponses           = 798
```

```
  snmpInTraps                  = 0
  snmpOutTraps                 = 0
From RFC2572
  snmpUnknownSecurityModels    = 0
  snmpInvalidMsgs              = 0
  snmpUnknownPDUHandlers       = 0
From RFC2573
  snmpUnavailableContexts      = 0
  snmpUnknownContexts          = 1
From RFC2574
  usmStatsUnsupportedSecLevels = 0
  usmStatsNotInTimeWindows     = 1
  usmStatsUnknownUserNames     = 1
  usmStatsUnknownEngineIDs     = 0
  usmStatsWrongDigests         = 0
  usmStatsDecryptionErrors     = 0
```

output definitions

From RFCxxxx	Displays the RFC number that defines the SNMP MIB objects listed.
MIB Objects	Name of the MIB object listed as an SNMP statistic.
= (integer)	The number of times the MIB object has been reported to the SNMP management station since the last reset.

Release History

Release 7.1.1; command was introduced.

Related Commands

snmp security	Configures the SNMP security settings.

MIB Objects

```
N/A
```

show snmp mib-family

Displays SNMP MIB information. Information includes MIP ID number, MIB table name, and command family.

show snmp mib-family [*table_name***]**

Syntax Definitions

table_name	The name of the MIB table to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- If a table name is not specified in the command syntax, all MIB table names will be displayed.
- If the command family is not valid for the entire MIB table, the command family will be displayed on a per-object basis.
- Table names are case-sensitive. Therefore, use the exact table names from the MIB database.

Examples

```
-> show snmp mib-family trapStationTable
MIP ID   MIB TABLE NAME                          FAMILY
-------+---------------------------------------+--------------------
 73733   trapStationTable                        snmp
```

output definitions

MIP ID	Identification number for the MIP associated with this MIB Table.
MIB Table Name	Name of the MIB table.
Family	Command family to which this MIB table belongs.

Release History

Release 7.1.1; command was introduced.

Related Commands

show snmp-trap filter-ip	Displays the SNMP trap filter information.

MIB Objects

N/A

snmp-trap absorption

Enables or disables the trap absorption function.

snmp-trap absorption {enable | disable}

Syntax Definitions

enable	Enables SNMP trap absorption. When trap absorption is enabled, identical, repetitive traps sent by applications during a pre-configured time period will be absorbed, and therefore not sent to SNMP Manager stations configured on the switch.
disable	Disables SNMP trap absorption.

Defaults

By default, trap absorption is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To view the current trap absorption status, use the **show snmp-trap config** command.

Examples

```
-> snmp-trap absorption enable
-> snmp-trap absorption disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show snmp-trap config	Displays the SNMP trap information. Information includes trap ID numbers and corresponding trap names and families.

MIB Objects

```
trapFilterTable
   trapAbsorption
```

snmp-trap to-webview

Enables the forwarding of traps to WebView.

snmp-trap to-webview {enable | disable}

Syntax Definitions

enable	Enables WebView forwarding. When WebView forwarding is enabled, all traps sent by switch applications are also forwarded to WebView. This allows a WebView session to retrieve the trap history log.
disable	Disables WebView forwarding.

Defaults

By default, WebView forwarding is enabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To view the current WebView forwarding status, use the **show snmp-trap config** command.

Examples

```
-> snmp-trap to-webview enable
-> snmp-trap to-webview disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show snmp-trap config	Displays the SNMP trap information, including the current status for trap absorption and WebView forwarding.

MIB Objects

```
trapFilterTable
   trapToWebView
```

snmp-trap replay-ip

Replays stored traps from the switch to a specified SNMP station. This command is used to replay (to resend) traps on demand. This is useful in the event when traps are lost in the network.

snmp-trap replay-ip {*ip_address* | *ipv6_address* | *domain_name***} [***seq_id***]**

Syntax Definitions

ip_address	The IP address for the SNMP station to which traps will be replayed from the switch.
ipv6_address	The IPv6 address for the SNMP station to which traps will be replayed from the switch.
domain_name	A Fully Qualified Domain Name (FQDN) for the SNMP station to which traps will be replayed. Specify a domain name up to 255 characters in length.
seq_id	The sequence number from which trap replay will begin. Each trap sent by the switch to an SNMP station has a sequence number. The sequence number reflects the order in which the trap was sent to the SNMP station. For example, the first trap sent to an SNMP station has a sequence number of 1; the second trap has a sequence number of 2, etc. If no sequence number is entered, all stored traps are replayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **show snmp station** command on page page 65-6 to display the latest stored sequence number for each SNMP station.
- The switch replays traps in the same order that they were previously sent, beginning from the specified sequence number.
- When traps are replayed, the original dates on which the trap was issued, rather than the current dates are used.
- When an FQDN is specified with this command, the switch will resolve the domain name to an IP address. Make sure the domain name maps to a valid and reachable IP address.
- If the specified sequence number is lower than the oldest trap sequence number stored in the switch, the switch replays all stored traps.
- If the specified sequence number is equal to or greater than the oldest trap sequence number stored, the switch replays all stored traps from the specified sequence number up to the latest sequence number.
- If the specified sequence number is greater than the latest sequence number, no traps are replayed.

Examples

```
-> snmp-trap replay-ip 172.12.2.100
-> snmp-trap replay-ip 300::1
-> snmp-trap replay-ip upam.omnivista.com
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R1; *domain_name* parameter option added.

Related Commands

show snmp station	Displays the current SNMP station status.
show snmp-trap replay-ip	Displays the SNMP trap replay information.

MIB Objects

```
trapStationTable
   trapStationReplay
   trapStationNextSeq
alaTrapInetStationTable
   alaTrapInetStationReplay
   alaTrapInetStationNextSeq
```

snmp-trap filter-ip

Enables or disables SNMP trap filtering. Trap filtering is used to determine whether a trap or group of traps will be sent from the switch to a specified SNMP station.

snmp-trap filter-ip {*ip_address* **|** *ipv6_address* **|** *domain_name***}** *trap_id_list*

no snmp-trap filter-ip {*ip_address* | *ipv6_address* **|** *domain_name***}** *trap_id_list*

Syntax Definitions

ip_address	The IP address for the SNMP station for which trap filtering is enabled or disabled.
ipv6_address	The IPv6 address for the SNMP station for which trap filtering is enabled or disabled.
domain_name	A Fully Qualified Domain Name (FQDN) for the SNMP station for which trap filtering is enabled or disabled. Specify a domain name up to 255 characters in length.
trap_id_list	Specifies the trap(s) for which filtering is being enabled or disabled. Traps must be specified using the numeric trap ID. You can specify more than one trap in the command line; separate each trap ID with a space and no comma.

Defaults

By default, SNMP trap filtering is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- To *enable* trap filtering, use the syntax **snmp-trap filter-ip** *ip_address trap_id_list*.
- To *disable* trap filtering, use the syntax **no snmp-trap filter-ip** *ip_address trap_id_list*.
- When an FQDN is specified with this command, the switch will resolve the domain name to an IP address. Make sure the domain name maps to a valid and reachable IP address.
- When filtering is enabled, the specified trap(s) *will not* be sent to the SNMP station. When filtering is disabled, the specified traps *will* be sent to the SNMP station.
- To display a list of traps and their ID numbers, use the **show snmp-trap config** command.

Examples

```
-> snmp-trap filter-ip 172.1.2.3 1
-> snmp-trap filter-ip 172.1.2.3 0 1 3 5
-> snmp-trap filter-ip 300::1 1 3 4
-> snmp-trap filter-ip upam.omnivista.com 1 3 5
-> no snmp-trap filter-ip 172.1.2.3 1
-> no snmp-trap filter-ip 172.1.2.3 0 1 3 5
```

```
-> no snmp-trap filter-ip 300::1 1 3
-> no snmp-trap filter-ip upam.omnivista.com 1 3 5
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R1; *domain_name* parameter option added.

Related Commands

show snmp-trap filter-ip	Displays the current SNMP trap filter status.
show snmp-trap config	Displays the SNMP trap information, including trap ID numbers, trap names, command families, and absorption rate.

MIB Objects

```
trapFilterTable
   trapFilterStatus
alaTrapInetFilterTable
   alaTrapInetFilterStatus
```

snmp authentication-trap

Enables or disables SNMP authentication failure trap forwarding.

snmp authentication-trap {enable | disable}

Syntax Definitions

enable	Enables authentication failure trap forwarding. When enabled, the standard authentication failure trap is sent each time an SNMP authentication failure is detected.
disable	Disables authentication failure trap forwarding.

Defaults

By default, authentication failure trap forwarding is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> snmp authentication-trap enable
-> snmp authentication-trap disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show snmp authentication-trap	Displays the current authentication failure trap forwarding status.

MIB Objects

```
snmpGroup
   snmpEnableAuthenTraps
```

show snmp-trap replay-ip

Displays SNMP trap replay information.

show snmp-trap replay-ip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show snmp-trap replay-ip
ipAddress         : oldest replay number
--------------------------------------
199.199.101.200 :       1234
199.199.105.202 :        578
199.199.101.203 :       1638
199.199.101.204 :       2560
upam.omnivista.com:     1849
```

output definitions

IPAddress	IP address or Fully Qualified Domain Name (FQDN) of the SNMP station manager that replayed the trap.
Oldest Replay Number	Number of the oldest replayed trap.

Release History

Release 7.1.1; command was introduced.

Related Commands

snmp-trap replay-ip	Replays stored traps from the switch to a specified SNMP station.

MIB Objects

```
trapStationTable
   trapStationReplay
   trapStationNextSeq
alaTrapInetStationTable
   alaTrapInetStationReplay
   alaTrapInetStationNextSeq
```

show snmp-trap filter-ip

Displays the current SNMP trap filter status.

show snmp-trap filter-ip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

To display a list of traps and their ID numbers, use the **show snmp-trap config** command.

Examples

```
-> show snmp-trap filter-ip
ipAddress            trapId list
------------------------------------------------------------------------------
199.199.101.200 :    0   1   2   3
199.199.101.201 :    no filter
199.199.105.202 :    0   1   2   3   4   5   6   7   8   9  10  11  12  13  14
                     15  16  17  18  19
199.199.101.203 :    20  22  30
199.199.101.204 :    no filter
upam.omnivista.com : 1 3 5
```

output definitions

IPAddress	IP address or Fully Qualified Domain Name (FQDN) of the SNMP management station that recorded the traps.
TrapId List	Identification number for the traps being filtered.

Release History

Release 7.1.1; command was introduced.

Related Commands

snmp-trap filter-ip	Enables or disables SNMP trap filtering.
show snmp-trap config	Displays the SNMP trap information, including trap ID numbers, trap names, command families, and absorption rate.

MIB Objects

```
trapFilterTable
   trapFilterEntry
alaTrapInetFilterTable
   alaTrapInetFilterStatus
```

show snmp authentication-trap

Displays the current authentication failure trap forwarding status (i.e., enable or disable).

show snmp authentication-trap

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show snmp authentication-trap
snmp authentication trap = disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

snmp authentication-trap	Enables or disables SNMP authentication failure trap forwarding.

MIB Objects

```
sessionAuthenticationTrap
```

show snmp-trap config

Displays SNMP trap information. Information includes trap ID numbers, trap names, command families, and absorption rate. This command also displays the Enabled/Disabled status of SNMP absorption and the Traps to WebView service.

show snmp-trap config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show snmp-trap config
Absorption service : enabled
Traps to WebView : enabled
Id trapName                           family          absorption
--+-----------------------------------+---------------+------------
 0 coldStart                          chassis         15 seconds
 1 warmStart                          chassis         15 seconds
 2 linkDown                           interface       15 seconds
 3 linkUp                             interface       15 seconds
 4 authenticationFailure              snmp            15 seconds
 5 entConfigChange                    module          15 seconds
30 slPesudoCAMStatusTrap              bridge          15 seconds
31 slbTrapException                   loadbalancing   15 seconds
32 slbTrapConfigChanged               loadbalancing   15 seconds
33 slbTrapOperStatus                  loadbalancing   15 seconds
34 ifMauJabberTrap                    interface       15 seconds
35 sessionAuthenticationTrap          session         15 seconds
-------------------------------------------------------------------
```

output definitions

Id	Identification number for the trap.
Trap Name	Name of the trap.
Family	Family to which the trap belongs.
Absorption	Time needed for the trap to process.

Release History

Release 7.1.1; command was introduced.

Related Commands

show snmp mib-family	Displays SNMP MIB information.
snmp-trap absorption	Enables or disables the trap absorption function.
snmp-trap to-webview	Enables or disables the forwarding of SNMP traps to WebView.

MIB Objects

```
trapConfigTable
   trapConfigEntry
```

event-action

Triggers the specified script to run when the specified event occurs.

event-action {trap *trigger_string* **script** *script_string* | **script-time-limit** *num***}**

no event-action trap *name*

Syntax Definitions

trigger_string	The name of the trigger. In the case of a trap, this is the trap name.
script_string	The path and the name of the script to run.
num	The maximum amount of time a script can run (30-600).
name	The name of the trap to remove the event from.

Defaults

parameter	default
script-time-limit	60 seconds.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- If the prefix for the script is not **/flash/python**, the path will be assumed to be under that directory.
- Each event can only be assigned a single script but a script can be assigned to multiple events.
- Only users that have write privileges for the AAA partition management family can create scripts in the **/flash/python** directory.
- The **show snmp-trap config** command can be used to view the list of traps available on the switch.

Examples

```
-> event-action trap linkDown script /flash/python/link_event.py
-> event-action trap stpNewRoot script stp_event.py
```

Release History

Release 7.3.4; command was introduced.

Related Commands

show event-action	Shows the scripts and statistics associated with the events.

MIB Objects

```
alaEventActionTable
   alaEventActionType
   alaEventActionName
   alaEventActionScriptName
   alaEventActionRowStatus
```

show event-action

Displays the scripts and statistics associated with the events.

show event-action [statistics | trap *name* **[statistics]]**

Syntax Definitions

name	The name of the trap to display statistics for.
statistics	Displays the statistics for all configured events or a specific trap.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, except 6900-V72, 6900-C32

Usage Guidelines

In the case of a virtual-chassis, the event-script can be run independently on the Master or Slave chassis. The Master and slave chassis have separate launch counters and the script launch counter will not be synchronized across chassis.

Examples

```
-> show event-action

 type              name                   script  (/flash/python/…)
------+ ---------------------------------+-----------------------------
trap    linkDown                          link_event.py
trap    stpNewRoot                        stp_event.py
trap    sessionAuthenticationTrap         catchAll.py

-> show event-action statistics
                                                    Script             Launch
 Type                    Name                       Last Launched      Count
------+---------------------------------------+--------------------+----------
trap   linkDown                                 2014-10-23 13:45:34      2
```

output definitions

Type	The type of event trigger.
Name	The name of the event. In the case of a trap, this is the trap name.
Script	The name and location of the script associated with the event.
Script Last Launched	The date and time the script was last run.
Launch Count	The number of times the script has been launched by the event.

Release History

Release 7.3.4; command was introduced.

Related Commands

event-action	This command will cause the specified script to be run when the specified event occurs.

MIB Objects

```
alaEventActionTable
   alaEventActionType
   alaEventActionName
   alaEventActionScriptName
```

66 OmniVista Cirrus Commands

OmniVista Cirrus is a network management solution to deliver zero touch provisioning using cloud.

OmniVista Cirrus solution provides reduced costs, ease of devices provisioning and a unified wired/ wireless management from the cloud. The solution also provides an ability to identify each device uniquely and provide a freemium/premium solution based on the user policy.

Deployment of OmniVista Cirrus provides easy to use management and monitoring tools in a network and the ability to manage the network using devices ranging from workstations to smart phones.

MIB information for the OmniVista Cirrus commands is as follows:

Filename: ALCATEL-IND1-SYSTEM-MIB.mib
Module: alcatelIND1SystemMIB

A summary of the available commands is listed here.

cloud-agent admin-state

Enables or disables OmniVista Cirrus functionality globally for the switch.

cloud-agent admin-state {enable | disable | disable force | restart}

Syntax Definitions

enable	Enables OmniVista Cirrus for the switch.
disable	Disables OmniVista Cirrus for the switch.
disable force	Disables OmniVista Cirrus for the switch and disconnects from the VPN.
restart	Restart option implicitly triggers "**disable force**" followed by "**enabled**".

Defaults

By default, OmniVista Cirrus is globally enabled for the switch.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

- OmniVista Cirrus is globally enabled for the switch only when the switch boots up without a configuration file [*(vc)boot.cfg*] or the configuration file size is zero bytes.
- If the switch boots up with a configuration file, the feature is enabled only if the administrative state of OmniVista Cirrus is explicitly enabled using the **cloud-agent admin-state** command. Hence, the default value is disabled in this case.
- The switch must have access to the DHCP server in the customer network with zero configurations on the devices.
- If the OmniVista Cirrus administrative state is disabled at run-time, it will take effect only after a reboot.
- If the OmniVista Cirrus administrative state is enabled at run-time, it will immediately trigger call-home with the activation server, if a connection was not established prior to that.
- When the OmniVista Cirrus administrative state is disabled at run-time while the connection is in progress or established, it will not have any consequences on the switch. If **write memory** is issued, the switch will not call-home even if the switch reboots or has a takeover. However, if the discovery interval timer is running, the next call-home will be terminated.
- The restart option implicitly triggers the administrative states of **disable force** followed by **enabled**. This will enable a user to restart call-home from OmniVista Cirrus.
- If the switch is in an intermediate state (downloading an image from image server, pre-provisioning, write memory, flash syncro, call-home, etc.), the **cloud agent admin state disable force** will display an error message: "*OV Cloud agent is in progress. Please retry after some time.*"

Examples

```
-> cloud-agent admin-state enable
-> cloud-agent admin-state disable
```

Release History

Release 8.4.1 R03; command introduced.
Release 8.5R1; **restart** parameter added.

Related Commands

cloud-agent discovery-interval	Configures the time interval after which the switch will call-home the activation server, in case of any fatal error.
show cloud-agent status	Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

MIB Objects

```
ovCloudAgent
   ovCloudAgentAdminState
```

cloud-agent discovery-interval

Configures the time interval after which the switch will call-home to the activation server, in case of any error.

cloud-agent discovery-interval *minutes*

Syntax Definitions

minutes	The time interval to call-home after an error. The valid range is 2-3600 minutes.

Defaults

By default, the discovery interval is set to 30 minutes.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

- Call-home with the activation server will be immediately triggered when OmniVista Cirrus administrative state is enabled at run-time, if a connection was not established prior to that.
- When the OmniVista Cirrus administrative state is disabled at run-time while the connection is in progress or in an established connection, it will not have any consequences on the switch. If **write memory** is issued, the switch will not call-home even if the switch reboots or has a takeover. However, if the discovery interval timer is running, the next call home will be terminated.
- When trying to connect to the openVPN server, if the connection is not established in 90 seconds, the switch will move to an error state and will call home after the expiry of the discovery interval.

Examples

```
-> cloud-agent discovery-interval 60
-> cloud-agent discovery-interval 90
```

Release History

Release 8.4.1 R03; command introduced.

Related Commands

cloud-agent admin-state	Enables or disables OmniVista Cirrus functionality globally for the switch.
show cloud-agent status	Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

MIB Objects

```
ovCloudAgent
   ovCloudAgentDiscoveryInterval
```

cloud-agent remove-inconsistent-certificate

Removes the certificate received from the OmniVista Activation server on all units in the VC, if the certificate status is inconsistent.

cloud-agent remove-inconsistent-certificate

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

- When this command is issued, a waning is generated: "*This command may render the switch incapable of connecting with OV-Cloud if not used with caution. Confirm (Y/N):*"
- If accepted by pressing (Y) and the certificate status is not inconsistent, an error message is displayed: "*Certificate status is Consistent. Cannot delete certificate.*" The existing OmniVista Cirrus agent state machine will not be interrupted.

Examples

```
-> cloud-agent remove-inconsistent-certificate
```

Release History

Release 8.5R1; command introduced.

Related Commands

cloud-agent admin-state	Enables or disables OmniVista Cirrus functionality globally for the switch.
show cloud-agent status	Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

MIB Objects

```
ovCloudAgent
   ovCloudAgentRemoveInconsistentCertificate
```

show cloud-agent status

Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

show cloud-agent status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

- The command **show cloud-agent status** will be valid only if call-home is enabled. Else, only the default values, if present, will be displayed.
- DHCP address, DHCP IP address mask, Gateway, Activation URL, Proxy URL, Proxy IP will be displayed based on the DHCP response parameters received.
- DNS server, DNS domain will be displayed with the current DNS configuration in the switch, if call-home is enabled.

Examples

```
-> show cloud-agent status
Admin State                    : Enabled,
Activation Server State        : completeOK,
Device State                   : DeviceManaged,
Error State                    : None,
Cloud Group                    : pmrb98earnoc10,
DHCP Address                   : 135.254.171.88,
DHCP IP Address Mask           : 255.255.255.0,
Gateway                        : 135.254.171.1,
Activation Server              : activation.myovcloud.com:443,
NTP Server                     : 135.254.171.160,
DNS Server                     : 10.67.0.254,
DNS Domain                     : netaos.in,
Proxy Server                   : 192.168.70.226:8000,
VPN Server                     : pmrb98earnoc10.tenant.vpn.dev.myovcloud.com:443,
Preprovision Server            : pmrb98earnoc10.tenant.ovd.dev.myovcloud.com:80,
OV tenant                      : pingram999.ov.dev.ovcirrus.com:443,
VPN DPD Time (sec)             : 0,
Image Server                   : -,
Image Download Retry Count     : -,
Discovery Interval (min)       : 30,
Time to next Call Home (sec)   : -,
Call Home Timer Status         : Not-Running,
Discovery Retry Count          : 1
```

```
Certificate Status              : Consistent
```

Release History

Release 8.4.1 R03; command introduced.
Release 8.5R1; “Certificate Status” added in command display.

Related Commands

cloud-agent admin-state	Enables or disables OmniVista Cirrus functionality globally for the switch.
show cloud-agent vpn status	Displays the OmniVista Cirrus VPN status.

MIB Objects

```
ovCloudAgent
   ovCloudAgentAdminState
   ovCloudAgentDiscoveryInterval
   ovCloudAgentDeviceState
   ovCloudAgentTimeToNextCallhome
```

show cloud-agent vpn status

Displays the OmniVista Cirrus VPN status.

show cloud-agent vpn status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900

Usage Guidelines

N/A

Examples

```
-> show cloud-agent vpn status
   VPN status                     : Connected,
   VPN Assigned IP                : 10.8.0.4,
   VPN DPD time (sec)             : 600
```

output definitions

VPN Status	Refers to OmniVista Cirrus VPN status. The various VPN states are: • **Connecting**—OpenVPN's initial state • **Wait**—Waiting for initial response from server • **Auth**—Authenticating with server • **Get_Config**—Downloading configuration options from server • **Assign_IP**—Assigning IP address to virtual network interface • **Add_Routes**—Adding routes to system • **Connected**—Initialization sequence completed • **Reconnecting**—A restart has occurred • **Exiting**—A graceful exit is in progress
VPN Assigned IP	Displays the VPN server assigned IP for the VPN connection towards the OmniVista Cirrus.
VPN DPD time (sec)	Displays the VPN Dead Peer Detection (DPD) time value in seconds.

Release History

Release 8.4.1 R03; command introduced.

Related Commands

cloud-agent admin-state	Enables or disables OmniVista Cirrus functionality globally for the switch.
show cloud-agent status	Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

MIB Objects

```
ovCloudAgent
   ovCloudAgentDeviceState
   ovCloudAgentVpnStatus
```

67 OpenFlow Commands

OpenFlow is a communications interface defined between the control and forwarding layers that is used in a Software Defined Network (SDN). OpenFlow separates the control plane and the data plane in the switch. Traditionally, switches and routers have made decisions on where packets should travel based on rules local to the device. With OpenFlow, only the data plane exists on the switch itself, and all control decisions are communicated to the switch from a central Controller. The OmniSwitch can operate in AOS or OpenFlow mode, including a modified OpenFlow mode known as Hybrid mode.

MIB information for the Web Management commands is as follows:

Filename: ALCATEL-IND1-OPENFLOW-MIB.mib
Module: alcatelIND1OpenflowMIB

A summary of the available commands is listed here:

OpenFlow Commands	**openflow back-off-max** **openflow idle-probe-timeout** **openflow logical-switch** **openflow logical-switch controller** **openflow logical-switch interfaces** **show openflow** **show openflow logical-switch**

openflow back-off-max

Configures the maximum amount of time to wait between Controller connection attempts.

openflow back-off-max *seconds*

Syntax Definitions

seconds	The back-off-max value, in seconds. The valid range is from 0 - 60.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6860, 6900, except 6900-V72, 6900-C32

Usage Guidelines

If set to 0, setting is disabled.

Examples

```
-> openflow back-off-max 0
-> openflow back-off-max 32
-> openflow back-off-max 60
```

Release History

Release 7.3.4; command introduced

Related Commands

show openflow	Displays global OpenFlow configuration parameters.

MIB Objects

```
alaOpenflowGlobalMIBConfigObjects
   alaOpenflowGlobalBackoffMax
```

openflow idle-probe-timeout

Configures the idle probe timeout value.

openflow idle-probe-timeout *seconds*

Syntax Definitions

seconds	The idle probe timeout value, in seconds. The valid range is 1 - 60.

Defaults

parameter	default
seconds	15

Platforms Supported

OmniSwitch 6860, 6900, except 6900-V72, 6900-C32

Usage Guidelines

If set to 0, idle probing is disabled.

Examples

```
-> openflow idle-probe-timeout 0
-> openflow idle-probe-timeout 15
-> openflow idle-probe-timeout 60
```

Release History

Release 7.3.4; command introduced

Related Commands

show openflow	Displays global OpenFlow configuration parameters.

MIB Objects

```
alaOpenflowGlobalMIBConfigObjects
   alaOpenflowGlobalIdleProbeTimeout
```

openflow logical-switch

Configures an OpenFlow Logical Switch. An OpenFlow Logical Switch consists of a portion of the switch's resources that are managed by an OpenFlow Controller (or set of Controllers) via the OpenFlow Agent.

openflow logical-switch *name* **[probe-time** *num* | **failure-detect-time** *num* **| tcp-buffer-size** *num* **| dpid** *string***] [admin-state {enable | disable}] [mode {normal | api | pfc-channel}] [version {1.0 | 1.3.1}+] [learned-mac-update {enable | disable}] [vlan** *vlan_id***] [table-miss-action {drop | controller}**

no openflow logical-switch <*name*>

Syntax Definitions

name	The Logical Switch name (up to 32 characters).
probe-time *num*	Configures probe-time for a logical switch in the pfc-channel mode which will override the existing global idle-probe-time for sending echo-requests to the OpenFlow Controller. (1-60)
failure-detect-time *num*	Configures the failure-detect-time for a logical switch in the pfc-channel mode for detecting a disconnection to the OpenFlow Controller if there was no echo reply or message from the controller. (1-60)
tcp-buffer-size *num*	Configures the TCP buffer size for socket connection to OpenFlow controllers configured for the logical-switch in the pfc-channel mode (2–32).
dpid *string*	Configures a unique 8-byte Datapath Identifier (DPID) for a logical switch in pfc-channel mode. Value must be entered in hex format only (starting with 0x) and must be less than 8-bytes.
admin-state enable	Enables the Logical Switch.
admin-state disable	Disables the Logical Switch.
normal	Configures the Logical Switch to run in Normal Mode.
api	Configures the Logical Switch to run in Hybrid (API) Mode. Only one (1) Logical Switch can be configured in Hybrid Mode.
pfc-channel	Configures the Logical Switch for NEC pfc-channel mode.
1.0	Configures the Logical Switch to run OpenFlow Version 1.0.
1.3.1	Configures the Logical Switch to run OpenFlow Version 1.3.1.
learned-mac-update enable	Enables the forwarding of new source learned MAC addresses to a WLAN controller.
learned-mac-update disable	Disables the forwarding of new source learned MAC address to a WLAN controller.
vlan_id	The Default VLAN for all ports assigned to the Logical Switch. Traffic on this VLAN on these ports will not carry an 802.1q tag. Traffic on all other VLANs on these ports will carry an 802.1q tag. The valid range is 2 - 4093.
drop | controller	Configures whether packets are dropped or sent to the Controller when an OpenFlow Table Miss occurs.

Defaults

parameter	default
probe-time *num*	5 seconds
failure-detect-time *num*	4 seconds
tcp-buffer-size *num*	2 KB
dpid *string*	Top 16-bit unique index of logical switch and bottom 48 bits of router MAC
admin-state enable | disable	enable
normal | api	normal
1.0 | 1.3.1	1.0, 1.3.1
learned-mac-update enable | disable	disable
drop | controller	drop

Platforms Supported

OmniSwitch 6860, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Up to three (3) OpenFlow Logical Switches can be configured on an OmniSwitch.
- Use the **no** form of the command to delete an OpenFlow Logical Switch and all Controller/port configurations for that Logical Switch.
- When a Logical Switch is disabled, all Controllers for that Logical Switch are operationally disabled, and flows added by those Controllers are removed.
- In Normal Mode, the switch operates as per the OpenFlow standards. In Hybrid mode, OpenFlow operates as an interface through which the Controller may add over-ride policies to the switch much like QoS. In Hybrid mode, no traffic is forwarded to the Controller(s) and AOS operates normally.
- OpenFlow versions 1.0 and 1.3.1 are both enabled by default. At least one version must be enabled.
- “vlan” is not valid if the configured mode for the Logical Switch is API. An API Logical Switch implicitly operates on all ports, link aggregates, and VLANs not assigned to other OpenFlow Logical Switches.
- OpenFlow version 1.0 and 1.3.1 use TCP port 6633.
- Enabling learned MAC update only applies if the configured mode for the Logical Switch is API.

Examples

```
-> openflow logical-switch vswitch1
-> openflow logical-switch vswitch1 admin-state enable
-> openflow logical-switch vswitch1 mode normal version 1.0 vlan 5
-> openflow logical-switch vswitchnec mode pfc-channel
-> no openflow logical-switch vswitch1
```

Release History

Release 7.3.4; command introduced

Related Commands

show openflow logical-switch	Displays information about all of the configured OpenFlow Logical Switches.

MIB Objects

```
alaOpenflowLogicalSwitchTable
   alaOpenflowLogicalSwitch
   alaOpenflowLogicalSwitchAdminState
   alaOpenflowLogicalSwitchMode
   alaOpenflowLogicalSwitchVersions
   alaOpenflowLogicalSwitchVlan
   alaOpenflowLogicalSwitchLearnedMacUpdate
   alaOpenflowLogicalSwitchProbeTime
   alaOpenflowLogicalSwitchFailureDetectTime
   alaOpenflowLogicalSwitchDPID
   alaOpenflowLogicalSwitchTableMissAction
   alaOpenflowLogicalSwitchTCPBufferSizeTx
   alaOpenflowLogicalSwitchTCPBufferSizeRx
```

openflow logical-switch controller

Configures a Controller for an OpenFlow Logical Switch. You can configure up to three (3) Controllers per Logical Switch.

openflow logical-switch *name* **controller {***ip_address* **|** *domain_name***} [***:port***] [priority** *num***] admin-state {enable | disable}**

no openflow logical-switch *name* **controller {***ip_address* **|** *domain_name***} [***:port***]**

Syntax Definitions

name	The Logical Switch name (up to 32 characters).
ip_address	The IP address of Controller.
domain_name	The Fully Qualified Domain Name (FQDN) of the Controller. Specify a domain name up to 255 characters in length.
port	The Controller IP Port (1 - 65535).
priority *num*	Configures the priority value for the specified Controller in pfc-channel mode (0-2). 0 = highest, 2 = lowest.
enable	Enables the connection to the Controller.
disable	Disables the connection to the Controller.

Defaults

parameter	default
port	6633
priority *num*	2
enable | disable	enable

Platforms Supported

OmniSwitch 6860, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Use the **no** form of this command to remove a Controller for a Logical Switch.
- Specify either the IPv4 address or the FQDN for the Controller. When an FQDN is specified, the switch will resolve the IP address for that domain.
- If a Logical Switch cannot connect to any of its Controllers, it runs in “Fail Secure Mode”. All flow aging, etc., continues unaffected while the Controllers are disconnected.
- Use the priority parameter to configure the priority for the specified Controller. If Controllers have the same priority, the one configured first will have priority.

Examples

```
-> openflow logical-switch vswitch1 controller 1.2.3.4
```

```
-> openflow logical-switch vswitch1 controller 1.2.3.4:6634
-> openflow logical-switch vswitch1 controller 1.2.3.4:6634 admin-state disable
-> openflow logical-switch vswitch1 controller 1.2.3.4:6634 priority 1
-> openflow logical-switch vswitchnec controller opendaylight.abc.com
-> openflow logical-switch vswitchnec controller opendaylight.abc.com:6635
-> openflow logical-switch vswitchnec controller opendaylight.abc.com:6635 disable
-> openflow logical-switch vswitchnec controller opendaylight.abc.com priority 1
-> no openflow logical-switch vswitch1 controller 1.2.3.4
-> no openflow logical-switch vswitchnec controller opendaylight.abc.com
```

Release History

Release 7.3.4; command introduced.
Release 8.5R1; *domain_name* parameter option added.

Related Commands

show openflow logical-switch	Displays information about all of the configured OpenFlow Logical Switches.

MIB Objects

```
alaOpenflowControllerTable
   alaOpenflowControllerLogicalSwitch
   alaOpenflowControllerIpType
   alaOpenflowControllerIp
   alaOpenflowControllerPort
   alaOpenflowControllerAdminState
   alaOpenflowControllerPriority
```

openflow logical-switch interfaces

Configures a range of interfaces to/from a Logical Switch.

openflow logical-switch *name* **interfaces {port** *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***] | [type {trunk | access}] | [native-vlan** *vlan***] | [vlan-tag** *vlan***[**-*vlan2***]]}**

no openflow logical-switch *name* **interfaces {port** *chassis/slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

Syntax Definitions

name	The Logical Switch name (up to 32 characters).
*chassis/slot/port***[**-*port2***]**	The chassis ID, slot, and port number.
*agg_id***[**-*agg_id2***]**	The link aggregate ID number.
trunk	Configures the interface type as trunk.
access	Configures the interface type as access.
native-vlan *vlan*	The default VLAN for an interface in the logical switch. Traffic on this port will be untagged for the native VLAN. Traffic on all other VLANs on this port will be tagged. (2-4093)
vlan-tag *vlan*[-vlan2]	The list of allowed tagged VLANs for an interface. Traffic on these allowed VLAN(s) of the ports and Untagged traffic will not carry an 802.1q tag. Traffic on all other VLANs on the port will be dropped. (2-4093)

Defaults

parameter	default
type	**access**

Platforms Supported

OmniSwitch 6860, 6900, except 6900-V72, 6900-C32

Usage Guidelines

The **native-vlan** and **vlan-tag** parameters are valid only if the logical switch mode is pfc-channel.

Examples

```
-> openflow logical-switch vswitch1 interfaces port 1/1/1
-> no openflow logical-switch vswitch1 interfaces port 1/1/1
-> openflow logical-switch vswitch2 interfaces linkagg 5
-> no openflow logical-switch vswitch2 interfaces linkagg 5
-> openflow logical-switch vswitch1 interfaces port 1/1/1-8
-> no openflow logical-switch vswitch1 interfaces port 1/1/1-8
-> openflow logical-switch vswitchnec interfaces port 1/1/20 type trunk
-> openflow logical-switch vswitchnec interfaces port 1/1/20 native-vlan 3
-> openflow logical-switch vswitchnec interfaces port 1/1/20 vlan-tag 4-5
```

Release History

Release 7.3.4; command introduced

Related Commands

show openflow logical-switch Displays information about all of the configured Logical Switches.

MIB Objects

```
alaOpenflowInterfaceTable
   alaOpenflowInterfaceLogicalSwitch
   alaOpenflowInterface
```

show openflow

Displays global OpenFlow configuration parameters.

show openflow

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6900, except 6900-V72, 6900-C32

Usage Guidelines

N/A

Examples

```
-> show openflow
Back-off Max       : 60,
Idle Probe Timeout : 15
```

output definitions

Back-off Max	The configured maximum back off time, in seconds, for Controller connection attempts (Range = 1 - 60, Default = 60).
Idle Probe Timeout	The configured idle probe timeout value, in seconds (Range = 1– 60, Default = 15).

Release History

Release 7.3.4; command introduced

Related Commands

openflow back-off-max	Configures the maximum amount of time allowed for Controller connection attempts.
openflow idle-probe-timeout	Configures the idle probe timeout value.

MIB Objects

```
alaOpenflowGlobalBackoffMax
alaOpenflowGlobalIdleProbeTimeout
```

show openflow logical-switch

Displays information about configured OpenFlow Logical Switches.

show openflow logical-switch [*name* **| controllers | interfaces [vlans | port | linkagg] | details]**

Syntax Definitions

name	The Logical Switch name (up to 32 characters).
controllers	The controllers assigned to this logical switch.
interfaces	The interfaces assigned to this logical switch.
details	The details of the logical switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6860, 6900, except 6900-V72, 6900-C32

Usage Guidelines

- Enter a Logical Switch name to display only information about a specific Logical Switch.
- The DPID, TCP-Buffer-Size, Probe-Time, and Failure-Detect-Time are only applicable for a logical switch in PFC mode.

Examples

```
-> show openflow logical-switch
                     Admin                                Learn
   Logical Switch    State  Mode    Versions    VLAN   MAC   Ctrlrs   Intf   Flows
--------------------+-----+------+-----------+------+-----+--------+------+-------
vswitch1             Ena   Norm   1.0             1  Dis         1      4       0
vswitch2             Dis   Norm   1.0, 1.3.1      5  Dis         3      4       2
vswitchnec           Ena   PFC    1.0, 1.3.1    N/A  Dis         1      0       0
```

output definitions

Logical Switch	The Logical Switch name
Admin State	The Logical Switch administrative state (Enabled or Disabled).
Mode	The Logical Switch operational Mode (Normal/API/PFC).
Versions	The OpenFlow versions enabled on the Logical Switch (1.0/1.3.1).
VLAN	The default VLAN for all ports assigned to the Logical Switch. Zero (0) indicates no VLAN configured.
Learn MAC	Whether new source learned MAC addresses are forwarded to a WLAN controller (Enabled or Disabled).

output definitions

Ctrlrs	The number of Controllers configured for the Logical Switch (up to three (3) Controllers can be configured per Logical Switch.
Intf	The number of interfaces (ports and link aggregations) configured for the Logical Switch.
Flows	The number of flows pushed to the Logical Switch by its Controllers.

```
-> show openflow logical-switch controllers
                                                                  Admin    Oper
        Logical Switch                Controller          Role    State    State
------------------------------+----------------------+----------+-----+---------
vswitch1                        192.168.2.9:6633        Master     Ena   Disconn
vswitch2                        192.168.2.9:6633        Master     Ena   Disabled
vswitch2                        192.168.2.10:6633       Equal      Dis   Disabled
vswitch2                        192.168.2.10:6634       Equal      Ena   Active
vswitch2                        192.168.2.9:6634        Slave      Ena   Idle
vswitchnec                      opendaylight.abc.com:66 Master     Ena   Active
```

output definitions

Logical Switch	The Logical Switch name
Controller	The Controller IP address or Fully Qualified Domain Name (FQDN) and port. If the FQDN is longer than 22 characters, the name may appear truncated in this field.
Role	Current role of the Controller (Equal, Master, or Slave).
Admin State	The Logical Switch administrative state (Enabled or Disabled).
Oper State	Current connection state of the Controller (invalid, operDisabled, sendError, init, connecting, backoff, exchangingHello, active, idle, disconnected).

```
-> show openflow logical-switch interfaces
        Logical Switch             Interface     Mode    Type
------------------------------+---------------+-------+--------
vswitch1                        1/1/1         Norm
vswitch2                        1/1/2         Norm
vswitch2                        1/1/3         Norm
vswitch2                        1/1/5         Norm
vswitch2                        1/1/10        Norm
vswitchnec                      1/1/5         PFC     Access
vswitchnec                      0/5           PFC     Access
```

output definitions

Logical Switch	The Logical Switch name
Interface	The interface slot/port or link aggregate ID configured for the Logical Switch.
Mode	The Logical Switch operational Mode (Normal/API/PFC).
Type	The type of interface assigned to the logical switch (Access or Trunk). • Access interfaces support only untagged ports in the native VLAN. • Trunk interfaces support untagged ports in the native VLAN and tagged ports in other VLANs.

```
-> show openflow logical-switch vswitchnec details
Logical-Switch:    vswitchnec
  DPID                = 0x1234567890123456
  TCP-Buffer-Size     = 2 Kilobytes
  Probe-Time          = 5 Sec
  Failure-Detect-Time = 4 Sec
  Table-Miss-Action   = DROP
```

output definitions

Logical Switch	The Logical Switch name
DPID	The DPID configured for the logical switch.
TCP-Buffer-Size	TCP Send Buffer size for socket towards Controller for the logical switch.
Probe-Time	The probe-time configured for the logical switch name.
Failure-Detect-Time	The failure-detect-time configured for the logical switch.
Table-Miss-Action	The action taken when an OpenFlow Table Miss occurs (DROP or CONTROLLER).

Release History

Release 7.3.4; command introduced

Related Commands

openflow logical-switch	Configures an OpenFlow Logical Switch.
openflow logical-switch controller	Configures a Controller for an OpenFlow Logical Switch. You can configure up to three (3) Controllers per Logical Switch.
openflow logical-switch interfaces	Configures a range of interfaces to/from a Logical Switch.

MIB Objects

```
alaOpenflowLogicalSwitchTable
   alaOpenflowLogicalSwitch
   alaOpenflowLogicalSwitchAdminState
   alaOpenflowLogicalSwitchMode
   alaOpenflowLogicalSwitchVersions
   alaOpenflowLogicalSwitchVlan
   alaOpenflowLogicalSwitchControllerCount
   alaOpenflowLogicalSwitchInterfaceCount
   alaOpenflowLogicalSwitchFlowCount
   alaOpenflowLogicalSwitchLearnedMacUpdate
   alaOpenflowLogicalSwitchProbeTime
   alaOpenflowLogicalSwitchFailureDetectTime
   alaOpenflowLogicalSwitchDPID
   alaOpenflowLogicalSwitchTableMissAction
   alaOpenflowLogicalSwitchTCPBufferSize
```

68 DNS Commands

A Domain Name System resolver is an internet service that translates host names into IP addresses. Every time you use a host name, a DNS service must resolve the name to an IP address. You can configure up to three domain name servers. If the primary DNS server does not know how to translate a particular host name, it asks the secondary DNS server (if specified). If this fails, it asks the third DNS server (if specified), until the correct IP address is returned (resolved). If all DNS servers have been queried and the name is still not resolved to an IP address, the DNS resolver will fail and issue an error message.

MIB information for the DNS commands is as follows:

Filename: ALCATEL-IND1-SYSTEM.mib
Module: alcatelIND1SystemMIB

A summary of the available commands is listed here.

ip domain-lookup

Enables or disables the DNS resolver.

ip domain-lookup

no ip domain-lookup

Syntax Definitions

N/A

Defaults

By default, the DNS resolver is disabled.

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to disable the DNS resolver.
- You must use the **ip domain-name** command to set a default domain name for your DNS resolver(s) and the **ip name-server** command to specify up to three DNS servers to query on host lookups.
- The **ip domain-lookup** command enables the DNS resolver.

Examples

```
-> ip domain-lookup
-> no ip domain-lookup
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip name-server	Specifies the IP addresses of up to three servers to query on a host lookup.
ipv6 name-server	Specifies the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.
ip domain-name	Sets or deletes the default domain name for DNS lookups.
show dns	Displays the current DNS resolver configuration and status.

MIB Objects

```
systemDNS
   systemDNSEnableDnsResolver
```

ip name-server

Specify the IP addresses of up to three servers to query on a host lookup.

ip name-server *server_address1* **[***server_address2* **[***server_address3***]]**

Syntax Definitions

server_address1	The IP address of the primary DNS server to query for host lookup. This is the only address that is required.
server_address2	The IP address of the secondary DNS server to query for host lookup. This server will be queried only if the desired host name or host IP address is not located by the primary DNS server. A second IP address is optional.
server_address3	The IP address of the DNS server with the lower priority. This server will be queried only if the desired host name or IP address is not located by the primary and secondary DNS servers. A third IP address is optional

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Configuration of the DNS resolver to resolve any host query requires that you first set the default domain name with the **ip domain-name** command and enable the DNS resolver function with the **ip domain-lookup** command before you specify the IP addresses of the DNS servers by using the **ip name-server** command.
- You can configure up to three IPv4 DNS servers and three IPv6 DNS servers in a switch.

Examples

```
-> ip name-server 189.202.191.14 189.202.191.15 188.255.19.1
-> ip name-server 10.255.11.66
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip domain-name	Sets or deletes the default domain name for DNS lookups.
show dns	Displays the current DNS resolver configuration and status.

MIB Objects

```
systemDNS
   systemDNSNsAddr1
   systemDNSNsAddr2
   systemDNSNsAddr3
```

ipv6 name-server

Specifies the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.

ipv6 name-server *server_ipv6_address1* **[***server_ipv6_address2* **[***server_ipv6_address3***]]**

Syntax Definitions

server_ipv6_address1	The IPv6 address of the primary IPv6 DNS server to query for host lookup. Specifying the primary IPv6 DNS address is mandatory.
server_ipv6_address2	The IPv6 address of the secondary IPv6 DNS server to query for host lookup. This server will be queried only if the desired host name is not able to be resolved by the primary IPv6 DNS server. A second IPv6 address is optional.
server_ipv6_address3	The IPv6 address of the IPv6 DNS server with the lower priority. This server will be queried only if the desired host name is not able to be resolved by both the primary and secondary IPv6 DNS servers. A third IPv6 address is optional.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Configuration of the DNS resolver to resolve any host query requires that you first set the default domain name with the **ip domain-name** command and enable the DNS resolver function with the **ip domain-lookup** command before you specify the IPv6 addresses of the IPv6 DNS servers by using the **ipv6 name-server** command.
- You cannot use multicast, loopback, link-local and unspecified IPv6 addresses for specifying IPv6 DNS servers.
- You can configure up to three IPv6 DNS servers and three IPv4 DNS servers in a switch.

Examples

```
-> ipv6 name-server fec0::2d0:d3:f3fc
-> ipv6 name-server fe2d::2c f302::3de1:1 f1bc::202:fd40:f3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip domain-name	Sets or deletes the default domain name for DNS lookups.
show dns	Displays the current DNS resolver configuration and status.

MIB Objects

```
systemDNS
   systemDNSNsIPv6Addr1
   systemDNSNsIPv6Addr2
   systemDNSNsIPv6Addr3
```

ip domain-name

Sets or deletes the default domain name for DNS lookups.

ip domain-name *name*

no ip domain-name

Syntax Definitions

name	The default domain name for host lookups.

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

- Use the **no** form of this command to delete the default domain name.
- Use this command to set the default domain name for DNS lookups.

Examples

```
-> ip domain-name company.com
-> no ip domain-name
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip name-server	Specifies the IP addresses of up to three servers to query on a host lookup.
ipv6 name-server	Specifies the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.
show dns	Displays the current DNS resolver configuration and status.

MIB Objects

```
systemDNS
   systemDNSDomainName
```

show dns

Displays the current DNS resolver configuration and status.

show dns

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6465, 6560, 6860, 6865, 6900, 9900

Usage Guidelines

N/A

Examples

```
-> show dns
Resolver is       : enabled
domainName        : company.com
IPv4 nameServer(s): 189.202.191.14
                  : 189.202.191.15
                  : 188.255.19.1
IPv6 nameServer(s): fe2d::2c
                  : f302::3de1:1
                  : f1bc::202:fd40:f3
```

output definitions

Resolver is	Indicates whether the DNS resolver is enabled or disabled.
domainName	Indicates the default domain name assigned to the DNS lookups. This value is set using the **ip domain-name** command.
IPv4 nameServer(s)	Indicates the IP address(es) of the IPv4 DNS server(s). These addresses are set using the **ip name-server** command.
IPv6 nameServer(s)	Indicates the IPv6 address(es) of the IPv6 DNS server(s). These addresses are set using the **ipv6 name-server** command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip name-server	Specifies the IP addresses of up to three servers to query on a host lookup.
ipv6 name-server	Specify the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.
ip domain-name	Sets or deletes the default domain name for DNS lookups.

MIB Objects

```
systemDNS
   systemDNSEnableDnsResolver
   systemDNSDomainName
   systemDNSNsAddr1
   systemDNSNsAddr2
   systemDNSNsAddr3
   systemDNSNsIPv6Addr1
   systemDNSNsIPv6Addr2
   systemDNSNsIPv6Addr3
```

A Software License and Copyright Statements

This appendix contains ALE USA, Inc. and third-party software vendor license and copyright statements.

ALE USA, Inc. License Agreement

ALE USA, INC. SOFTWARE LICENSE AGREEMENT

IMPORTANT. Please read the terms and conditions of this license agreement carefully before opening this package.

By opening this package, you accept and agree to the terms of this license agreement. If you are not willing to be bound by the terms of this license agreement, do not open this package. Please promptly return the product and any materials in unopened form to the place where you obtained it for a full refund.

1. **License Grant.** This is a license, not a sales agreement, between you (the "Licensee") and ALE USA, Inc. ALE USA, Inc. hereby grants to Licensee, and Licensee accepts, a non-exclusive license to use program media and computer software contained therein (the "Licensed Files") and the accompanying user documentation (collectively the "Licensed Materials"), only as authorized in this License Agreement. Licensee, subject to the terms of this License Agreement, may use one copy of the Licensed Files on the Licensee's system. Licensee agrees not to assign, sublicense, transfer, pledge, lease, rent, or share their rights under this License Agreement. Licensee may retain the program media for backup purposes with retention of the copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Licensed Materials or any portions thereof may be made by Licensee and Licensee shall not modify, decompile, disassemble, reverse engineer, or otherwise attempt to derive the Source Code. Licensee is also advised that ALE USA, Inc. products contain embedded software known as firmware which resides in silicon. Licensee may not copy the firmware or transfer the firmware to another medium.

2. **ALE USA, Inc.'s Rights.** Licensee acknowledges and agrees that the Licensed Materials are the sole property of ALE USA, Inc. and its licensors (herein "its licensors"), protected by U.S. copyright law, trademark law, and are licensed on a right to use basis. Licensee further acknowledges and agrees that all rights, title, and interest in and to the Licensed Materials are and shall remain with ALE USA, Inc. and its licensors and that no such right, license, or interest shall be asserted with respect to such copyrights and trademarks. This License Agreement does not convey to Licensee an interest in or to the Licensed Materials, but only a limited right to use revocable in accordance with the terms of this License Agreement.

3. **Confidentiality.** ALE USA, Inc. considers the Licensed Files to contain valuable trade secrets of ALE USA, Inc., the unauthorized disclosure of which could cause irreparable harm to ALE USA, Inc.. Except as expressly set forth herein, Licensee agrees to use reasonable efforts not to disclose the Licensed Files to any third party and not to use the Licensed Files other than for the purpose authorized by this License Agreement. This confidentiality obligation shall continue after any termination of this License Agreement.

4. **Indemnity.** Licensee agrees to indemnify, defend and hold ALE USA, Inc. harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation ALE USA, Inc.'s reasonable United States and local attorneys' and expert witnesses' fees and costs) arising out of or in connection with the unauthorized copying, marketing, performance or distribution of the Licensed Files.

5. **Limited Warranty.** ALE USA, Inc. warrants, for Licensee's benefit alone, that the program media shall, for a period of ninety (90) days from the date of commencement of this License Agreement (referred to as the Warranty Period), be free from defects in material and workmanship. ALE USA, Inc. further warrants, for Licensee benefit alone, that during the Warranty Period the Licensed Files shall operate substantially in accordance with the functional specifications in the User Guide. If during the Warranty Period, a defect in the Licensed Files appears, Licensee may return the Licensed Files to ALE USA, Inc. for either replacement or, if so elected by ALE USA, Inc., refund of amounts paid by Licensee under this License Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE LICENSED MATERIALS ARE LICENSED "AS IS" AND ALE USA, INC. AND ITS LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. THIS WARRANTY GIVES THE LICENSEE SPECIFIC LEGAL RIGHTS. LICENSEE MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

6. **Limitation of Liability.** ALE USA, Inc.'s cumulative liability to Licensee or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the license fee paid to ALE USA, Inc. for the Licensed Materials. IN NO EVENT SHALL ALE USA, INC. BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF ALE USA, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION TO INCIDENTAL OR CONSEQUENTIAL DAMAGES MAY NOT APPLY TO LICENSEE.

7. **Export Control.** This product is subject to the jurisdiction of the United States. Licensee may not export or reexport the Licensed Files, without complying with all United States export laws and regulations, including but not limited to (i) obtaining prior authorization from the U.S. Department of Commerce if a validated export license is required, and (ii) obtaining "written assurances" from licensees, if required.

8. **Support and Maintenance.** Except as may be provided in a separate agreement between ALE USA, Inc. and Licensee, if any, ALE USA, Inc. is under no obligation to maintain or support the copies of the Licensed Files made and distributed hereunder and ALE USA, Inc. has no obligation to furnish Licensee with any further assistance, documentation or information of any nature or kind.

9. **Term.** This License Agreement is effective upon Licensee opening this package and shall continue until terminated. Licensee may terminate this License Agreement at any time by returning the Licensed Materials and all copies thereof and extracts therefrom to ALE USA, Inc. and certifying to ALE USA, Inc. in writing that all Licensed Materials and all copies thereof and extracts therefrom have been returned or erased by the memory of Licensee's computer or made non-readable. ALE USA, Inc. may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by

ALE USA, Inc., Licensee agrees to return to ALE USA, Inc. or destroy the Licensed Materials and all copies and portions thereof.

10. **Governing Law.** This License Agreement shall be construed and governed in accordance with the laws of the State of California.

11. **Severability.** Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms herein.

12. **No Waiver.** The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

13. **Notes to United States Government Users.** Software and documentation are provided with restricted rights. Use, duplication or disclosure by the government is subject to (i) restrictions set forth in GSA ADP Schedule Contract with ALE USA, Inc.'s reseller(s), or (ii) restrictions set forth in subparagraph (c) (1) and (2) of 48 CFR 52.227-19, as applicable.

14.**Third Party Materials.** Licensee is notified that the Licensed Files contain third party software and materials licensed to ALE USA, Inc. by certain third party licensors. Some third party licensors are third part beneficiaries to this License Agreement with full rights of enforcement. Please refer to the section entitled "Third Party Licenses and Notices" on page -4 for the third party license and notice terms.

Third Party Licenses and Notices

Legal Notices applicable to any software distributed alone or in connection with the product to which this document pertains, are contained in files within the software itself located at: **/flash/foss**.

Also, if needed, we provide all FOSS (Free and Open Source Software) source code used in this release at the following URL: https://github.com/Alcatel-LucentEnterpriseData.

CLI Quick Reference

Ethernet Port Commands

interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} {admin-state | autoneg | epp} {enable | disable}
interfaces {slot *chassis/slot* | port *chassis/slot/port* **[**-*port2***]**} speed {10 | 100 | 1000 | 2500 | 10000 | 40000 | 100000 | 2000 | 4000 | 8000 | auto | max {100 | 1000 | 4000 | 8000}}
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} crossover {auto | mdix | mdi}
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} duplex {full | half | auto}
interfaces port *chassis/slot/port* alias *description*
clear interfaces {slot *chassis/slot* | port *chassis/slot/port*[-*port2*} {l2-statistics [cli] | tdr-statistics}
interfaces {slot *chassis/slot* | port *chassis/slot/port*[-*port2*} max-frame-size *bytes*
interfaces {slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]**} inter-frame-gap bytes
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} flood-limit {bcast | mcast | uucast | all} rate {pps *pps_num*| mbps *mbps_num* | cap% *cap_num* | enable | disable | default} [low-threshold *low_num*]
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} flood-limit {bcast | mcast | uucast | all} action {shutdown | trap | default}
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} ingress-bandwidth {mbps| enable | disable}
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} pause {tx | rx | tx-and-rx | disable}
interfaces [slot *chassis/slot* | port *chassis/slot/port* **[**-*port2*]] link-trap {enable | disable}
interfaces ddm {enable | disable}
interfaces ddm-trap {enable | disable}
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} wait-to-restore *num*
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} wait-to-shutdown *num*
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} eee {enable | disable}
interfaces primary-port *chassis/slot/port* split-mode {auto | 4X25G | 4X10G | 40G | 100G}
interfaces {slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]**} fec {disable | auto | fc | rs}
interfaces {slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]**} hybrid-mode {fiber | copper}
interfaces port *chassis/slot/port***[**-*port2***]** loopback
no interfaces port *chassis/slot/port***[**-*port2***]** loopback
clear violation {port *chassis/slot/port***[**-*port2***]** | linkagg *agg_id***[**-*agg_id2***]}**
violation recovery-maximum {infinite | *max_attempts}*
violation [slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]]** recovery-maximum {infinite | default | *max_attempts}*
violation recovery-time seconds
violation [slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]]** recovery-time {seconds | default}
violation recovery-trap {enable | disable}
show interfaces [slot *chassis/slot* | port *chassis/*slot/*port*[-*port2*]]
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] alias
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] status
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] capability
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] accounting
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] counters
show interfaces [slot *chassis/slot* | port *chassis/*slot/*port*[-*port2*]] counters errors
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] flood-rate
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] traffic
show interfaces **[**slot *chassis/slot*| port *chassis/slot/port***[**-*port1***]]** ingress-rate-limit
show interfaces **[**slot *chassis/slot*| port *chassis/slot/port***[**-*port1***]]** ddm [w-low | w-high | status | a-low | a-high | actual]
show interfaces **[**slot *chassis/slot* | port *chassis/slot/port***[**-*port1***]]** split-mode
show transceivers [slot chassis/slot [transceiver transceiver_num]]
show violation [port *chassis/slot/port***[**-*port2***]** | linkagg *agg_id***[**-*agg_id2***]**]
show violation-recovery-configuration {slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]**}
interfaces {slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]**} link-monitoring admin-status {enable | disable}
interfaces {slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]**} link-monitoring time-window *seconds*
interfaces {slot *chassis/slot* | port *chassis/slot/port***[**-*port2***]**} link-monitoring link-flap-threshold *link_flaps*
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} link-monitoring link-error-threshold *mac_errors*
interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} clear-link-monitoring-stats
show interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} link-monitoring config
show interfaces {slot *chassis/slot*| port *chassis/slot/port***[**-*port2***]**} link-monitoring statistics
interfaces port chassis/slot/port tdr enable
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] tdr-statistics
link-fault-propagation group group_id [admin-status {enable | disable}]
no link-fault-propagation group {group_id[-*group_id2*]**}**
link-fault-propagation group group_id source {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]}
no link-fault-propagation group group_id source {port *chassis/slot/port***[**-*port2***]** | linkagg *agg_id***[**-*agg_id2***]**}
link-fault-propagation group group_id destination {port *chassis/slot/port[-port2]* | linkagg *agg_id[-agg_id2]*}
no link-fault-propagation group group_id destination {port *chassis/slot/port[-port2]* | linkagg *agg_id[-agg_id2]*}
link-fault-propagation group group_id wait-to-shutdown seconds
show link-fault-propagation group [group_id**]**
interfaces {slot *chassis/slot* | port *chassis/slot/port*[-*port2]*} beacon [admin-status {enable | disable}] [led-color color] [led-mode {solid | activity}]
no interfaces {slot *chassis/slot* | port *chassis/slot/port*[-*port2]*} beacon
show interfaces [slot *chassis/slot* | port *chassis/slot/port*[-*port2*]] beacon

interfaces ptp admin-state {enable | disable} [loopback-portlist <*chassis/slot/port*> <*chassis/slot/port*>] [*chassis/slot/port*] [priority {*num* | default}]
interfaces port *chassis/slot/port* ptp p2p admin-state {enable | disable}
show interfaces ptp config
interfaces {slot *chassis/slot*| port *chassis/slot/port* [*-port2*]} macsec admin-state {enable | disable} [mode {static sci-rx [*hex-num*] key-chain *keychain_id* [encryption] sci-tx [*hex-num]* key-chain *keychain_id* [encryption] | dynamic {keychain *cak_keychain_id* [server-priority *priority*] | radius}} [transmit-interval *tx_interval*] [encryption]]
no interfaces {slot *chassis/slot*| port *chassis/slot/port* [*-port2*]} macsec [sci-rx [*hex-num*] [sci-tx] [keychain] [encryption]
show interfaces macsec [*chassis/slot/port* [*-port2*]
show interfaces macsec static [*chassis/slot/port* [*-port2*]
show interfaces macsec dynamic [details] [*chassis/slot/port* [*-port2*]
show interfaces macsec statistics [*chassis/slot/port* [*-port2*]
clear interfaces {slot *chassis/slot* | port [*chassis/slot/port* [*-port2*] |all} macsec-statistics

Power over Ethernet (PoE) Commands

lanpower {*chassis* chassis | *slot* chassis/slot } service {*start* | *stop*}
lanpower port chassis/slot/port admin-state {*enable* | *disable*}
lanpower *{chassis chassis | slot chassis/slot | port chassis/slot/port}* type *string*
lanpower {slot chassis/slot | port chassis/slot/port} power milliwatts
lanpower {chassis chassis | slot chassis/slot | port chassis/slot/port} power milliwatts
lanpower {chassis chassis | slot chassis/slot } maxpower watts
lanpower *{chassis chassis | slot chassis/slot | port chassis/slot/port}* priority {critical | high | low}
lanpower *{chassis chassis | slot chassis/slot } ni*-priority {critical | high | low}
lanpower *{chassis chassis | slot chassis/slot*} priority-disconnect {enable | disable}
lanpower power-rule rule-name [admin-state {enable | disable}] [power {on | off}] [at {minutes mm | time hh:mm}] [days {all | day [day...] | date [date...]} [months {all | month}] [timezone {local-server | utc | originator-server}]
no lanpower power-rule rule-name [admin-state {enable | disable}] [power {on | off}] [at {minutes mm | time hh:mm}] [days {all | day [day...] | date [date...]} [months {all | month}] [timezone {local-server | utc | originator-server}]
lanpower *[slot chassis/slot | port chassis/slot/port-port]* power-policy policy-name [power-rule rule-name]
no lanpower power-policy name
lanpower {chassis *chassis* | slot *chassis/slot*} class-detection {enable | disable}
lanpower {chassis *chassis* | slot *chassis/slot*} capacitor-detection {enable | disable}
lanpower {chassis *chassis* | slot *chassis/slot*} usage-threshold *num*
lanpower {chassis *chassis* | slot *chassis/slot*} dynamic-power-management {enable | disable}
lanpower slot {*chassis/slot* | *all}* update-from *filename*
lanpower {slot *chassis/slot* | *port chassis/slot/port-port}* 4pair {enable | disable}
lanpower {slot *chassis/slot* | *port chassis/slot/port-port}* power-over-hdmi {enable | disable}
lanpower {slot *chassis/slot}* 802.3bt {enable | disable}
show lanpower slot *chassis/slot*
show lanpower power-rule [*name*]
show lanpower power-policy [policy-name slot | policy-name power-rule | policy-name port]
show lanpower {chassis chassis | slot chassis/slot } class-detection
show lanpower {chassis chassis | slot chassis/slot } capacitor-detection
show lanpower {chassis chassis | slot chassis/slot } priority-disconnect
show lanpower {chassis chassis | slot chassis/slot } ni-priority
show lanpower {chassis chassis | slot chassis/slot } usage-threshold]
show lanpower slot {chassis/slot | all} update-from

UDLD Commands

udld {enable | disable}
udld port chassis/slot/port[*-port2*] {enable | disable}
udld [port [chassis/slot/port[*-port2*]] mode {normal | aggressive}
udld [port [*chassis*/slot/port[*-port2*]] probe-timer seconds
no udld [port [*chassis*/slot/port[*-port2*]] probe-timer
udld [port [*chassis*/slot/port[*-port2*]] echo-wait-timer seconds
no udld [port [*chassis*/]slot/port[*-port2*]] echo-wait-timer
clear udld statistics [port *chassis*/slot/port]
show udld configuration
show udld configuration port [*chassis*/slot/port]
show udld statistics port *chassis*/slot/port
show udld neighbor port *chassis*/slot/port
show udld status port [*chassis/slot/port*]

Source Learning Commands

mac-learning {vlan *vlan[-vlan2]* | port *chassis/slot/port*[*-port2*] | linkagg *agg_id*} {enable | disable}
mac-learning flush {dynamic | static | multicast} [mac-address *mac_address*]
mac-learning flush domain all {dynamic | static}
mac-learning flush domain vlan {vlan *vlan_id*} {port *chassis/slot/port* | linkagg *agg_id*} | {dynamic | static | static-multicast} [mac-address *mac_address*]
mac-learning flush domain spb {serviceid *service_id* | sap *chassis/slot/port:encap* | bind-sdp *sdp_id*[:*service_id*] | isid *instance_id*} {dynamic | static} [mac-address *mac_address*]
mac-learning flush domain vxlan {serviceid *service_id* | sap *chassis/slot/port:encap* | bind-sdp *sdp_id*[:*service_id*] | vnid *vxlan_id*} {dynamic | static} [mac-address *mac_address*]
mac-learning flush domain l2gre {serviceid *service_id* | sap *chassis/slot/port:encap* | bind-sdp *sdp_id*[:*service_id*] | vpnid *vpn_id*} {dynamic | static} [mac-address *mac_address*]
mac-learning flush domain local serviceid *service_id* [sap *chassis/slot/port:encap*] static [mac-address *mac_address*]

mac-learning {vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}} static mac-address *mac_address* [bridging | filtering]
mac-learning flush [vlan *vlan_id* [port *chassis/slot/port* | linkagg *agg_id*]] static [mac-address *mac_address*]
mac-learning domain vlan vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*} static mac-address *mac_address* [bridging | filtering]
mac-learning flush domain vlan [vlan *vlan_id* [port *chassis/slot/port* | linkagg *agg_id*]] static [mac-address *mac_address*]
mac-learning domain spb {serviceid *service_id* {isid *instance_id* | sap *chassis/slot/port:encap* | bind-sdp *sdp_id*:*service_id*} static mac-address *mac_address* [bridging | filtering]
mac-learning domain spb {isid *instance_id* {sap *chassis/slot/port:encap* | bind-sdp *sdp_id*:*service_id*} static mac-address *mac_address* [bridging | filtering]
mac-learning flush domain spb {serviceid *service_id* | sap *chassis/slot/port:encap* | bind-sdp *sdp_id*[:*service_id*] | isid *instance_id*} static [mac-address *mac_address*]
mac-learning domain vxlan {serviceid *service_id* {sap *chassis/slot/port:encap* | vnid *vxlan_id* [sap *chassis/slot/port:encap*]} static mac-address *mac_address* [bridging | filtering]
mac-learning domain vxlan vnid *vxlan_id* sap *chassis/slot/port:encap* static mac-address *mac_address* [bridging | filtering]
mac-learning flush domain vxlan {serviceid *service_id* | sap *chassis/slot/port:encap* | bind-sdp *sdp_id*[:*service_id*] | vnid *vxlan_id*} static [mac-address *mac_address*]
mac-learning domain local serviceid *service_id* sap *chassis/slot/port:encap* static mac-address *mac_address* [bridging | filtering]
mac-learning flush domain local serviceid *service_id* [sap *chassis/slot/port:encap*] static [mac-address *mac_address*]
mac-learning {vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id* }} multicast mac-address *multicast_address* [group *group_id*]
mac-learning flush [vlan *vlan_id* [port *chassis/slot/port* | linkagg *agg_id*]] multicast [mac-address *multicast_address*]
mac-learning aging-time {*seconds* | default}
no mac-learning aging-time
mac-learning mode [centralized | distributed]
show mac-learning [summary | dynamic | static | multicast | bmac] [port *chassis/slot/port*] [linkagg *agg_id*] [mac-address *mac_address*] [remote [mac-address *mac_address*]]
show mac-learning domain all [summary]
show mac-learning domain vlan [vlan *vlan_id*] [port *chassis/slot/port* | linkagg *agg_id*] [dynamic | static | static-multicast | bmac] [mac-address *mac_address*] [summary]
show mac-learning domain spb [isid *instance_id* | serviceid *service_id* [isid *instance_id*]] [sap *chassis/slot/port:encap* | bind-sdp *sdp_id*[:*service_id*]] [dynamic | static] [mac-address *mac_address*] [summary]
show mac-learning domain vxlan [vnid *vxlan_id* | serviceid *service_id* [vnid *vxlan_id*]] [sap *chassis/slot/port:encap* | bind-sdp *sdp_id*[:*service_id*]] [dynamic | static] [mac-address *mac_address*] [summary]
show mac-learning domain l2gre {serviceid *service_id* | sap *chassis/slot/port:encap* | bind-sdp *sdp_id*[:*service_id*] | vpnid *vpn_id*} {dynamic | static} [mac-address *mac_address*] [summary]
show mac-learning domain local [serviceid *service_id*] [sap *chassis/slot/port:encap* | dynamic | static | mac-address *mac_address*] [summary]
show mac-learning aging-time
show mac-learning learning-state [vlan *vlan***[***-vlan2***]** | port *chassis/slot/port* | linkagg *agg_id***]**
show mac-learning mode
mac-ping dst-mac mac_address vlan vlan_id [priority vlan_priority] [drop-eligible {true | false}] [count count] [interval delay] [size size] [isid-check isid]

VLAN Management Commands

vlan *vlan_id* [admin-state {enable | disable}] [name *description***]**
no vlan *vlan_id*
vlan *vlan_id*[*-vlan_id]* members {port *chassis/slot/port[-port1]* | linkagg *agg_id***[***-agg_id***]**}
untagged
no vlan *vlan_id*[*-vlan_id]* members {port *chassis/slot/port[-port1]*| linkagg *agg_id***[***-agg_id***]**}
vlan *vlan_id*[*-vlan_id*] members {port chassis/slot/port[-port] | linkagg *agg_id***[***-agg_id***]**}
tagged
no vlan *vlan_id*[*-vlan_id*] members {port chassis/slot/port[-port] | linkagg *agg_id***[***-agg_id***]**}
vlan *vlan_id* mtu-ip *size*
show vlan [*vlan_id*]
show vlan [*vlan_id*[*-vlan_id*]] members [port *chassis/slot/port*[*-port*]| linkagg *agg_id*[*-agg_id*]]
pvlan *vlan_id*[-vlan_id] [admin-state {enable | disable}] [name *description***]** mtu-ip *size*
no pvlan *vlan_id*[- vlan_id]
pvlan *vlan_id* secondary vlan_id[-vlan_id] type {isolated | community}
no pvlan *vlan_id secondary vlan_id*[- vlan_id]
pvlan *vlan_id* members {port *chassis/slot/port[-port]* | linkagg *agg_id*[*-agg_id*]} {tagged | untagged} | isl}
no pvlan *vlan_id* members {port *chassis/slot/port[-port]* | linkagg *agg_id*[*-agg_id*]}
show pvlan [*vlan_id***[***-vlan_id]***]**
show pvlan [vlan_id] mapping
show pvlan [*vlan_id***[***-vlan_id***]**] members

High Availability VLAN Commands

server-cluster *cluster_id* [name *cluster_name*] [mode {L2 | L3}] [admin-state {enable | disable}]
no server-cluster *cluster_id*
server-cluster *cluster_id* vlan *vlan_id*
server-cluster *cluster_id* mac-address *mac_address*
server-cluster *cluster_id* ip *ip_address* [mac-address {static *mac_address* | dynamic}]

server-cluster *cluster_id* igmp-mode {enable | disable}
server-cluster *cluster_id* ip-multicast *ipm_address*
server-cluster *cluster_id* port {*chassis/slot/port*[-*port2*] | all}
no server-cluster *cluster-id* port {*chassis/slot/port*[-*port2*] | all}
server-cluster *cluster_id* linkagg *agg_id*[-*agg_id2*]
no server-cluster *cluster_id* linkagg *agg_id*[-*agg_id2*]}
show server-cluster [*cluster_id* [port]]

VLAN Stacking Commands

ethernet-service svlan {svlan_id[-svlan_id2]} [admin-state {enable | disable}] [name *description*]
no ethernet-service svlan {svlan_id [-svlan_id2]}
ethernet-service service-name *service_name* svlan *svlan_id*
no ethernet-service service-name *service_name* svlan *svlan_id*
ethernet-service nni {port chassis/slot/port [-port2] | linkagg agg_id[-agg_id2]} [tpid *tpid_value*] [[stp | mvrp] legacy-bpdu {enable | disable}]
no ethernet-service nni {port chassis/slot/port [-port2] | linkagg agg_id[-agg_id2]}
ethernet-service svlan {svlan_id[-svlan_id2]} nni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
no ethernet-service svlan {svlan_id[-svlan_id2]} nni {port chassis/slot/port[-*port2*] | linkagg agg_id[-agg_id2]}
ethernet-service sap *sap_id* service-name *service_name*
no ethernet-service sap sap_id
ethernet-service sap sap_id uni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
no ethernet-service sap sap_id uni {port chassis/slot/port[-*port2*] | linkagg agg_id[-agg_id2]}
ethernet-service sap sap_id cvlan {all | *cvlan_id*[-*cvlan_id2*] | untagged}
no ethernet-service sap sap_id cvlan {all | *cvlan_id*[-*cvlan_id2*] | untagged}
ethernet-service sap-profile *sap_profile_name* [bandwidth not-assigned] [[shared | not-shared] ingress-bandwidth *mbps*] [cvlan-tag {preserve | translate}] priority [not-assigned | map-inner-to-outer-p | map-dscp-to-outer-p | fixed *value*][egress-bandwidth *mbps*]
no ethernet-service sap-profile *sap_profile_name*
ethernet-service sap *sap_id* sap-profile *sap_profile_name*
no ethernet-service sap *sap_id*
ethernet-service uni-profile *uni_profile_name [tunnel-mac mac_address]* [l2-protocol *protocol*] {peer | discard | tunnel | mac-tunnel}
no ethernet-service uni-profile *uni_profile_name*
ethernet-service uni-profile *uni_profile_name* inbound {tagged | untagged | both} l2-protocol 802.1ab {peer | discard | tunnel}
no ethernet-service uni-profile *uni_profile_name*
ethernet-service uni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} uni-profile uni_profile_name
ethernet-service custom-L2-protocol custom_protocol_name mac mac_address [mask mask | ethertype ethertype [subtype subtype] | ssap/dsap ssap/dsap pid pid]
no ethernet-service custom-L2-protocol name
ethernet-service uni-profile *uni_profile_name custom-L2-protocol* custom_protocol_name {tunnel | discard | mac-tunnel}
no ethernet-service uni-profile *uni_profile_name custom-L2-protocol* custom_protocol_name
ethernet-service mac-tunneling {enable | disable}
ethernet-service svlan svid1[-svid2] mac-tunneling {enable | disable}
ethernet-service transparent-bridging [nni port chassis/slot/port[-port2] | nni linkagg agg_id[-agg_id2] {enable | disable}]
show ethernet-service vlan [vlan_id-[vlan_id2]]
show ethernet-service [service-name *service_name* | svlan svlan_id | transparent-bridging]
show ethernet-services sap [*sap_id*]
show ethernet-service port {*chassis/slot/port* | linkagg agg_id}
show ethernet-service nni [port *chassis/slot/port* | linkagg agg_id]
show ethernet-services nni [port *chassis/slot/port* | linkagg agg_id] l2pt-statistics
clear ethernet-services nni [port chassis/slot/port[-port2] | linkagg *agg_id*[-*agg_id2*]] l2pt-statistics
show ethernet-service uni [port *chassis/slot/port* | linkagg agg_id]
show ethernet-service uni [port *chassis/slot/port* | linkagg agg_id] l2pt-statistics
clear ethernet-service uni [port chassis/slot/port[-port2] | linkagg *agg_id*[-*agg_id2*]] l2pt-statistics
show ethernet-service uni-profile [*uni_profile_name*]
show ethernet-service custom-l2-profile [custom_protocol_name]
show ethernet-service uni-profile [*uni_profile_name*] l2pt-statistics
clear ethernet-service uni-profile [uni_profile_name] l2pt-statistics
show ethernet-service mac-tunneling
show ethernet-service sap-profile *sap_profile_name*
loopback-test *profile_name* destination-mac *dest_address {*port *chassis/slot/port* | linkagg *agg_id}* source-mac *src_address* vlan *vlan_id {*type {inward | outward [sap *sap_id]*}]
loopback-test *profile_name* admin-state {enable | disable}
no loopback-test *profile_name*
show loopback-test [*profile_name*] [counters]
clear loopback-test counters

Distributed Spanning Tree Commands

spantree mode {flat | per-vlan}
spantree [cist | vlan *vlan_id*] protocol {stp | rstp | mstp}
spantree vlan *vlan_id* [-*vlan_id2*] admin-state {enable | disable}
spantree mst region name *name*
no spantree mst region name
spantree mst region revision-level *rev_level*
spantree mst region max-hops *max_hops*

spantree msti *msti_id* [name *name*]
no spantree msti *msti_id* [name]
spantree msti *msti_id* vlan *vlan_id*[-*vlan_id2*]
no spantree msti *msti_id* vlan *vlan_id*[-*vlan_id2*]
spantree [cist | msti *msti_id* | vlan *vlan_id*] [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] priority *priority*
spantree [cist | vlan *vlan_id*] hello-time *seconds*
spantree [cist | vlan *vlan_id*] max-age *seconds*
spantree [cist | vlan *vlan_id*] forward-delay seconds
spantree {vlan *vlan_id* | cist} bpdu-switching {enable | disable}
spantree path-cost-mode {auto | 32bit}
spantree pvst+compatibility {port *chassis/slot/port*] | linkagg *agg_id*} {enable | disable | auto}
spantree [msti *msti_id*] auto-vlan-containment {enable | disable}
spantree cist {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} {enable | disable}
spantree vlan *vlan_id [-vlan2]* {port *chassis/slot/port[-port2]* | linkagg *agg_id[-agg_id2*]} {enable | disable}
spantree cist {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} path-cost *path_cost*
spantree msti *msti_id* {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} path-cost *path_cost*
spantree vlan *vlan_id* {port *chassis/slot/port*[-*port2*] | linkagg *agg_id* [-*agg_id2*]} path-cost *path_cost*
spantree cist {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} mode {forwarding | dynamic | blocking}
spantree {port *chassis/slot/port*[-*port2*] | linkagg *linkagg_id* [-*linkagg_id2*]} loop-guard {enable | disable}
spantree vlan *vlan_id* {port *chassis/slot/port*[-*port2*] | linkagg *agg_id* [-*agg_id2*]} mode {dynamic | blocking | forwarding}
spantree cist {port *chassis/slot/port* [-*port2*] | linkagg *agg_id* [-*agg_id2*]} connection {noptp | ptp | autoptp}
spantree vlan *vlan_id* {port *chassis/slot/port* [-*port2*] | linkagg *agg_id* [-*agg_id2*]} connection {noptp | ptp | autoptp}
spantree cist {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} admin-edge {enable | disable}
spantree vlan *vlan_id* {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} admin-edge {enable | disable}
spantree cist {port *chassis/slot/port*[-*port2*] | linkagg *agg_id* [-*agg_id2*]} auto-edge {enable | disable}
spantree vlan *vlan_id* {port *chassis/slot/port*[-*port2*] | linkagg *agg_id* [-*agg_id2*]} auto-edge {enable | disable}
spantree cist {port *chassis/slot/port[-port2]* | *linkagg agg_id[-agg_id2]*} restricted-role {enable | disable}
spantree vlan *vlan_id* {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} restricted-role {enable | disable}
spantree cist {port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} restricted-tcn {enable | disable}
spantree vlan *vlan_id* {port *chassis/slot/port* [-*port2*] | linkagg *agg_id* [-*agg_id2*]} restricted-tcn {enable | disable}
spantree cist txholdcount *value*
spantree vlan *vlan_id* txholdcount {*value*}
show spantree
show spantree cist
show spantree msti [*msti_id*]
show spantree vlan [*vlan_id*]
show spantree ports [forwarding | blocking | active | configured]
show spantree cist ports [forwarding | blocking | active | configured]
show spantree msti [*msti_id*] ports [forwarding | blocking | active | configured]
show spantree vlan [*vlan_id*[-*vlan_id2*]] ports [forwarding | blocking | active | configured]
show spantree mode
show spantree mst {region | port *chassis/slot/port* | linkagg *agg_id*}
show spantree msti [*msti_id*] vlan-map
show spantree cist vlan-map
show spantree [vlan *vlan_id*] map-msti

Shortest Path Bridging Commands

spb bvlan {*bvlan_id*[-*bvlan_id2*]} [admin-state {enable | disable}] [name *description*]
no spb bvlan *bvlan_id*
spb isis bvlan *bvlan_id* ect-id *ect_id*
spb isis control-bvlan *bvlan_id*
spb isis bvlan *bvlan_id* tandem-multicast-mode {sgmode | gmode}
spb isis bridge-priority *priority*
spb isis interface {port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]} [admin-state {enable | disable} [hello-interval *seconds*] [hello-multiplier *count*] [metric *metric*]
no spb isis interface [port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]]
spb ipvpn bind vrf {*vrf_name* | default} isid *instance_id* gateway *ip_address* {all-routes | import-route-map *route_map_name*}
no spb ipvpn bind vrf {*vrf_name* | default} isid *instance_id* gateway *ip_address*
spb ipvpn redist {source-vrf {*vrf_name* | default} | source-isid *instance_id*} destination-isid *instance_id* {all-routes | route-map *route_map_name*}
no spb ipvpn redist {source-vrf *vrf_name* | source-isid *instance_id*} destination-isid *instance_id*
show spb ipvpn bind [vrf {*vrf_name* | default}] [isid *instance_id*]
show spb ipvpn redist [vrf | [isid]
show spb ipvpn route-table [isid *instance_id*]
spb ipvpn6 bind vrf {*vrf_name* | default} isid *instance_id* gateway *ipv6_address* {all-routes | import-route-map *route_map_name*}
no spb ipvpn6 bind vrf {*vrf_name* | default} isid *instance_id* gateway *ipv6_address*

spb ipvpn6 redist {source-vrf {*vrf_name* | default} | source-isid *instance_id*} destination-isid *instance_id* {all-routes | route-map *route_map_name*}
no spb ipvpn6 redist {source-vrf *vrf_name* | source-isid *instance_id*} destination-isid *instance_id*
show spb ipvpn6 bind [vrf {*vrf_name* | default}] [isid *instance_id*]
show spb ipvpn6 redist [vrf | [isid]
show spb ipvpn6 route-table [isid *instance_id*]
spb isis admin-state {enable | disable}
spb isis area-address *area_address*
spb isis source- id {*source_id* | auto}
spb isis control-address {alll1 | alll2 | allis}
spb isis spf-wait [initial-wait *milliseconds* | second-wait *milliseconds*| max-wait *milliseconds*]
spb isis lsp-wait {max-wait *milliseconds* | initial-wait *milliseconds* | second-wait *milliseconds*}
spb isis rapid-lsp-converge {isid *instance_id* | admin-state {enable | disable}}
spb isis overload [timeout *seconds*]
no spb isis overload
spb isis overload-on-boot [timeout *seconds*]
no spb isis overload-on-boot
spb isis graceful-restart
no spb isis graceful-restart
spb isis graceful-restart helper {enable | disable}
show spb isis info
show spb isis interface
show ip isis adjacency [detail]
show ip isis database [lsp-id *lsp_id*]
show spb isis nodes
show spb isis unicast-table [bvlan *bvlan_id*]
show spb isis services [isid *instance_id* | bvlan *bvlan_id*]
show spb isis spf bvlan *bvlan_id* [bmac *mac_address*]
show spb isis multicast-table [isid *instance_id*]
show spb isis multicast-sources
show spb isis multicast-sources-spf bvlan *bvlan_id* bmac *mac_address* [dest *mac_address*]
show spb isis ingress-mac-filter [port chassis/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*] | bvlan *bvlan_id* | bmac *mac_address*]
show spb isis rapid-lsp-converge-info
show spb isis rapid-lsp-converge-table

Service Manager Commands

service *service_id*[-*service_id2*] spb isid *instance_id*[-*instance_id2*] bvlan *bvlan_id*[*:x*]
no service *service_id* spb
service *service_id*[-*service_id2*] vxlan vnid {*vxlan_id*[-*vxlan_id2*] | *xxx.xxx.xxx*[-*xxx.xxx.xxx*]}
no service *service_id* vxlan
service *service_id* l2gre vpnid {*vpn_id*}
no service *service_id* l2gre
service {*service_id* | all} description *desc_info*
no service {*service_id* | all} description
service {*service_id* | all} multicast-mode {head-end | tandem | hybrid}
service {*service_id* | all} stats {enable | disable}
service {*service_id* | all} vlan-xlation {enable | disable}
service {*service_id* | all} admin-state {enable | disable}
service *service_id* remove-ingress-tag {enable | disable}
service vxlan udp-port {*udp_port_num* | default}
service vxlan vrf {*vrf_name* | default}
service local-vrrp {enable | disable}
service l2gre reserved-vlan *vlan_id*[-*vlan_id2*]
no service l2gre reserved-vlan *vlan_id*[-*vlan_id2*]
service l2profile *l2profile_name* [stp | 802.1x | 802.3ad | 802.1ab | mvrp | gvrp | amap] [peer | drop | tunnel]
no service l2profile *profile-name*
service l2profile *l2profile_name* inbound {tagged |untagged | both} 802.1ab {peer | drop | tunnel}
no service l2profile *profile-name*
service access {port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]} [description *port_description*]
service access {port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]} no description
no service access {port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]}
service access {port *chassis*/*slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]} l2profile {default | *profile-name*}
service access {port *chassis*/*slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]} vlan-xlation {enable | disable}
service *service_id* sap {port *chassis*/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*]}
no service *service_id* sap {port chassis/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*]} [*sap_id*]
service *service_id* sap {port *chassis*/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*]} {:0 | :all | :*qtag*[-*qtag2*] | :outer_qtag.inner_qtag} description *desc_info*
no service *service_id* sap {port *chassis*/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*]} [:0 | :all | :*qtag*[-*qtag2*] | :outer_qtag.inner_qtag] description
service *service_id* sap {port *chassis*/slot/port | linkagg *agg_num*} [:0 | :all | :qtag | :outer_qtag.inner_qtag] {trusted | un-trusted [*priority*]}
service *service_id* sap {port *chassis*/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*]} {:0 | :all | *:qtag*[-*qtag2*] | :outer_qtag.inner_qtag} stats {enable | disable}
service *service_id* sap {port *chassis*/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*]} {:0 | :all | *:qtag*[-*qtag2*] | :outer_qtag.inner_qtag} admin-state {enable | disable}
service sdp *sdp_id* vxlan {far-end *ip_address* | multicast-group *mc_group_address*} [ttl {*ttl_num* | default}] [description *desc_info*] [admin-state {enable | disable}]

no service sdp *sdp_id* [description]
service sdp *sdp_id* l2gre far-end *ip_address* [ttl {*ttl_num* | default}] [description *desc_info*] [admin-state {enable | disable}]
no service sdp *sdp_id* [description]
service *service_id* bind-sdp *sdp_id1* [*sdp_id2 sdp_id3* ...] [description *desc_info*]
service *service_id*[-*service_id2*] bind-sdp *sdp_id* [description *desc_info*]
no service *service_id* bind-sdp *sdp_id* [description]
service l2gre auto-discover {enable | disable}
service rfp *rfp_id* local-endpoint *lep_id* [admin-state {enable | disable}] [ccm-interval {interval100ms | interval1s | interval10s | interval1m | interval10m | interval-invalid}] [level *number*] type spb
no service rfp *rfp_id* [local-endpoint *lep_id*]
service rfp *rfp_id* remote-endpoint *rep_id* service-id *service_id*[-*service_id2*]
no service rfp *rfp_id* remote-endpoint *rep_id* [service-id *service_id*[-*service_id2*]]
show service l2profile [*profile_name*]
show service access [port *chassis*/slot/port**[**-*port2***]** | linkagg *agg_id[-agg_id2*]] [sap]
show service [spb | vxlan | l2gre | *service_id*]
show service {*service_id* | isid *instance_id* | vnid *vxlan_id* | vpnid *vpn_id*} ports
show service spb *service_id* sap {port *chassis/slot/port* **|** linkagg *agg_num***}** [:0 | :all **|** :qtag1 | **:**outer_qtag.inner_qtag]
show service sdp [*sdp_id*]
show service sdp spb [sysid *mac_address* | bvlan *bvlan_id*]]
show service sdp vxlan [far-end *ip_address* | multicast-group *mc_group_address*]]
show service sdp l2gre [far-end *ip_address*]
show service bind-sdp [*sdp_id*[:*service_id*]]
show service bind-sdp [spb | isid *instance_id*]
show service bind-sdp [vxlan | vnid *vxlan_id*]
show service bind-sdp [l2gre | vpnid *vpn_id*]
show service {*service_id* | isid *instance_id* | vnid *vxlan_id* | vpnid *vpn_id*} debug-info
show service info
show service {*service_id* | vnid *vxlan_id* | vpnid *vpn_id*} counters
clear service [*service_id*] [sap {port *chassis*/slot/port | linkagg agg_id}[:0 | :all | :*qtag* | :*outer_qtag.inner_qtag*] | mesh-sdp *sdp_id*] counters
show service rfp [*rfp_id* [local-sap-status]]
show service rfp configuration [*rfp_id*]

Loopback Detection Commands

loopback-detection [remote-origin] {enable | disable}
loopback-detection port chassis/slot/port**[**-*port2***]** **[**remote-origin**]** {enable | disable}
loopback-detection service-access {port chassis/slot/port[-port2] | linkagg *agg_id[-agg_id2*]} {enable | disable}
loopback-detection transmission-timer seconds
loopback-detection autorecovery-timer seconds
show loopback-detection
show loopback-detection port [*chassis*/slot/port]
show loopback-detection linkagg agg_id
show loopback-detection statistics port *chassis*/slot/port
clear loopback-detection statistics port *[chassis*/slot/port]

Link Aggregation Commands

linkagg static agg *agg_id[-agg_id2*] size *size* [name *name*] [admin-state {enable | disable}] [multi-chassis active] [hash {source-mac | destination-mac | source-and-destination-mac | source-ip | destination-ip | source-and-destination-ip | tunnel-protocol}]
no linkagg static agg *agg_id[-agg_id2*]
linkagg static agg *agg_id[-agg_id2*] name *name*
no linkagg static agg *agg_id[-agg_id2*] name
linkagg static agg *agg_id[-agg_id2*] wait-to-restore-time *wtr_minutes*
no linkagg static agg *agg_id[-agg_id2*] wait-to-restore-time
linkagg static agg *agg_id[-agg_id2*] loopback
linkagg static agg *agg_id[-agg_id2*] loopback
linkagg static agg *agg_id[-agg_id2*] admin-state {enable | disable}
linkagg static port *chassis/slot/port***[**-*port2***]** agg *agg_id*
no linkagg static port *chassis/slot/port***[**-*port2***]**
linkagg lacp agg *agg_id[-agg_id2*] size *size*
no linkagg lacp agg *agg_id[-agg_id2*] size *size*
linkagg lacp agg *agg_id* name *name*
no linkagg lacp agg *agg_id[-agg_id2*] name
linkagg lacp agg *agg_id[-agg_id2*] wait-to-restore-time *wtr_minutes*
no linkagg lacp agg *agg_id[-agg_id2*] wait-to-restore-time
linkagg lacp agg *agg_id[-agg_id2*] admin-state {enable | disable}
linkagg lacp agg *agg_id[-agg_id2*] actor admin-key *actor_admin_key*
no linkagg lacp agg *agg_id[-agg_id2*] actor admin-key
linkagg lacp agg *agg_id[-agg_id2*] actor system-priority *actor_system_priority*
no linkagg lacp agg *agg_id[-agg_id2*] actor system-priority
no linkagg lacp agg *agg_id[-agg_id2*] actor system-id
linkagg lacp agg *agg_id[-agg_id2*] partner system-id *partner_system_id*
no linkagg lacp agg *agg_id[-agg_id2*] partner system-id
linkagg lacp agg *agg_id[-agg_id2*] partner system-priority *partner_system_priority*
no linkagg lacp agg *agg_id[-agg_id2*] partner system-priority
linkagg lacp agg *agg_id[-agg_id2*] partner admin-key *partner_admin_key*
no linkagg lacp agg *agg_id[-agg_id2*] partner admin-key
linkagg lacp port *chassis/slot/port*[-*port2*] actor admin-key *actor_admin_key*
no linkagg lacp port *chassis/slot/port*[-*port2*] [actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}]
linkagg lacp port *chassis/slot/port***[**-*port2***]** actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}

no linkagg lacp port *chassis/slot/port*[-*port2*] actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}
linkagg lacp port *chassis/slot/port*[-*port2*] actor system-id *actor_system_id*
no linkagg lacp port *chassis/slot/port*[-*port2*] actor system-id
linkagg lacp port *chassis/slot/port*[-*port2*] actor system-priority *actor_system_priority*
no linkagg lacp port *chassis/slot/port*[-*port2*] actor system-priority
linkagg lacp port *chassis/slot/port*[-*port2*] partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}
no linkagg lacp port *chassis/slot/port*[-*port2*] partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}
linkagg lacp port *chassis/slot/port*[-*port2*] partner admin system-id *partner_admin_system_id*
no linkagg lacp port *chassis/slot/port*[-*port2*] partner admin system-id
linkagg lacp port *chassis/slot/port*[-*port2*] partner admin-key *partner_admin_key*
no linkagg lacp port *chassis/slot/port*[-*port2*] partner admin-key
linkagg lacp port *chassis/slot/port*[-*port2*] partner admin system-priority *partner_admin_system_priority*
no linkagg lacp port *chassis/slot/port*[-*port2*] partner admin system-priority
linkagg lacp port *chassis/slot/port*[-*port2*] actor port-priority *actor_port_priority*
no linkagg lacp port *chassis/slot/port*[-*port2*] actor port-priority
linkagg lacp port *chassis/slot/port*[-*port2*] partner admin-port *partner_admin_port*
no linkagg lacp port *chassis/slot/port*[-*port2*] partner admin-port
linkagg lacp port *chassis/slot/port*[-*port2*] partner admin port-priority *partner_admin_port_priority*
no linkagg lacp port *chassis/slot/port*[-*port2*] partner admin port-priority
dhl *dhl_num [name name]*
no dhl *dhl_num*
dhl *dhl_num linka* {port chassis/slot/port | linkagg agg_id} *linkb* {port chassis/slot/port | linkagg agg_id}
no dhl *dhl_num linka* {port chassis/slot/port | linkagg agg_id} *linkb* {port chassis/slot/port | linkagg agg_id}
dhl *dhl_num admin-state* {enable | disable}
dhl *dhl_num vlan-map linkb {vlan_id[-vlan_id]}*
no dhl *dhl_num vlan-map linkb {vlan_id[-vlan_id]}*
dhl *dhl_num pre-emption-time seconds*
dhl *dhl_num mac-flushing* {none | raw | mvrp}
show dhl [*dhl_num*]
show dhl *dhl_num* [linkA | linkB]
linkagg *range local {agg_id-agg_id | none} peer {agg_id-agg_id | none}* multi-chassis *{agg_id-agg_id | none}*
show linkagg [agg *agg_id[-agg_id2*]]
show linkagg [agg *agg_id[-agg_id2*]] port [*chassis/slot/port*]
show linkagg accounting
show linkagg counters [errors]
show linkagg traffic
clear linkagg-statistics [agg *agg_id[-agg_id2*]]
show linkagg range [operation | config]

Virtual Chassis Commands

virtual-chassis [chassis-id *oper_chassis]* configured-chassis-id *config_chassis*
no virtual-chassis [chassis-id *oper_chassis]* configured-chassis-id *config_chassis*
virtual-chassis [chassis-id *oper_chassis]* chassis-group group
virtual-chassis [chassis-id *oper_chassis] configured*-chassis-priority priority
virtual-chassis [chassis-id *oper_chassis]* configured-control-vlan vlan
virtual-chassis [chassis-id *oper_chassis]* configured-hello-interval hello
virtual-chassis [chassis-id *oper_chassis]* vf-link vfl_id create
no virtual-chassis [chassis-id *oper_chassis]* vf-link vfl_id
virtual-chassis [chassis-id *oper_chassis]* vf-link vfl_id member-port [oper_chassis/]slot/port
no virtual-chassis [chassis-id *oper_chassis]* vf-link vfl_id member-port [oper_chassis/]slot/port
virtual-chassis [chassis-id *oper_chassis] vf-link vfl_id* default-vlan vlan
no virtual-chassis [chassis-id *oper_chassis] vf-link vfl_id* default-vlan
virtual-chassis [chassis-id *oper_chassis]* hello-interval hello
virtual-chassis shutdown [chassis-id *oper_chassis]*
virtual-chassis vf-link-mode {static | auto}
[no] virtual-chassis auto-vf-link-port chassis/slot/port
vc-takeover
convert configuration to *dir [reload]*
show virtual-chassis [chassis-id {oper_chassis}] topology
show virtual-chassis [chassis-id oper_chassis] consistency
show virtual-chassis [chassis-id *oper_chassis]* vf-link vfl_id member-port [oper_chassis/]slot/port
show virtual-chassis [chassis-id *oper_chassis]* auto-vf-link-port [*chassis/*slot/port]
show virtual-chassis [chassis-id oper_chassis] chassis-reset-list
show virtual-chassis [chassis-id oper_chassis] slot-reset-list
show virtual-chassis [chassis-id oper_chassis] neighbors
show configuration vcm-snapshot chassis-id oper_chassis
virtual-chassis split-protection admin-state {enable | disable}
virtual-chassis split-protection linkagg *agg_id*
no virtual-chassis split-protection linkagg
virtual-chassis split-protection guard-timer *time*
virtual-chassis split-protection helper admin-state {enable | disable}
virtual-chassis split-protection helper linkagg agg_id
no virtual-chassis split-protection helper linkagg
show virtual-chassis split-protection status
show virtual-chassis split-protection vc-units
show virtual-chassis split-protection helper status

Ethernet Ring Protection Commands

erp-ring ring_id port1 {*chassis/slot/port* | linkagg agg_id} port2 {*chassis/slot/port* | linkagg agg_id} service-vlan vlan_id level level_num [guard-timer *guard_timer*] [wait-to-restore-timer *wtr_timer*] [enable | disable]
no erp-ring ring_id
erp-ring ring_id rpl-node {port *chassis/slot/port* | linkagg agg_id}
no erp-ring ring_id rpl-node
erp-ring ring_id wait-to-restore wtr_timer
no erp-ring ring_id wait-to-restore
erp-ring ring_id {enable | disable}
erp-ring ring_id guard-timer guard_timer
no erp-ring ring_id guard-timer
erp-ring ring_id sub-ring-port {*chassis/slot/port* | linkagg agg_id} service-vlan vlan_id level level_num [guard-timer *guard_timer*] [wait-to-restore-timer *wtr_timer*] [enable | disable]
erp-ring ring_id virtual-channel [enable | disable]
erp-ring ring_id revertive [enable | disable]
erp-ring ring_id clear
erp-ring ring_id ethoam-event {*chassis/slot/port* | linkagg agg_id} remote-endpoint mep_id
no erp-ring ring_id ethoam-event {*chassis/slot/port* | linkagg agg_id}
clear erp statistics [ring ring_id [port *chassis/slot/port* | linkagg agg_id]]
show erp [ring ring_id | [port *chassis/slot/port* | linkagg agg_id]]
show erp statistics [ring ring_id [port *chassis/slot/port* | linkagg agg_id]]

MVRP Commands

mvrp {enable | disable}
mvrp port *chassis/slot/port*[–*port2*] {enable | disable}
mvrp linkagg *agg_id*[-*agg_id2*] {enable | disable}
mvrp maximum-vlan *vlan_limit*
mvrp {port *chassis/slot/port*[– *port2*] | linkagg *agg_id*[-*agg_id2*]} registration {normal | fixed | forbidden}
mvrp {port *chassis/slot/port*[–*port2*] | linkagg *agg_id*[-*agg_id2*]} applicant {participant | non-participant | active}
mvrp {port *chassis/slot/port***[–***port2***]** | linkagg *agg_id***[-***agg_id2***]}** timer join *timer_value*
mvrp {port *chassis/slot/port***[–***port2***]** | linkagg *agg_id***[-***agg_id2***]}** timer leave *timer_value*
mvrp {port *chassis/slot/port***[–***port2***]** | linkagg *agg_id***[-***agg_id2***]}** timer leaveall *timer_value*
mvrp {port *chassis/slot/port***[–** *port2***]** | linkagg *agg_id***[-***agg_id2***]}** timer periodic-timer *timer_value*
mvrp {port *chassis/slot/port***[–***port2***]** | linkagg *agg_id***[-***agg_id2***]}** periodic-transmission {enable | disable}
mvrp {port *chassis/slot/port* [– *port2*] | linkagg *agg_id*[-*agg_id2*]} restrict-vlan-registration vlan *vlan_list*
no mvrp {port *chassis/slot/port* [– *port2*] | linkagg *agg_id*[-*agg_id2*]} restrict-vlan-registration vlan *vlan_list*
mvrp {port *chassis/slot/port*[–*port2*] | linkagg *agg_id*[-*agg_id2*]} restrict-vlan-advertisement vlan *vlan_list*
no mvrp {port *chassis/]slot/port*[–*port2*] | linkagg *agg_id*[-*agg_id2*]} restrict-vlan-advertisement vlan *vlan_list*
mvrp {linkagg *agg_id*[-*agg_id2*] | port *chassis/slot/port*[–*port2*]} static-vlan-restrict vlan *vlan_list*
no mvrp {linkagg *agg_id*[-*agg_id2*] | port *chassis/slot/port*[–*port2*]} static-vlan-restrict vlan *vlan_list*
show mvrp configuration
show mvrp port [*chassis/slot/port*[-*port2*]] [enable | disable]
show mvrp linkagg [*agg_id*[-*agg_id2*]} [enabled | disabled]
show mvrp [port *chassis/slot/port***[–** *port2***]** | linkagg *agg_id***[-***agg_id2***]**] timer {join | leave | leaveall | periodic-timer}
show mvrp {port *chassis/slot/port***[–** *port2***]** | linkagg *agg_id***[-***agg_id2***]}** statistics
show mvrp {port *chassis/slot/port***[–** *port2***]** | linkagg *agg_id***[-***agg_id2***]}** last-pdu-origin
show mvrp {port *chassis/slot/port***[–** *port2***]** | linkagg *agg_id***[-***agg_id2***]}** vlan-restrictions
mvrp **[**port *chassis/slot/port* [–*port2*] | linkagg *agg_id*[-*agg_id2*]**]** clear-statistics

802.1AB Commands

lldp nearest-edge mode {enable | disable}
lldp transmit interval seconds
lldp transmit hold-multiplier num
lldp reinit delay seconds
lldp notification interval seconds
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port**[**-*port2***]** | slot chassis/slot | chassis} lldpdu {tx | rx | tx-and-rx | disable}
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port**[**-*port2***]** | slot chassis/slot | chassis} notification {enable | disable}
lldp network-policy policy_id application {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} vlan {untagged | priority-tag | vlan-id} [l2-priority 802.1p_value] [dscp dscp_value]
no lldp network-policy policy_id - [policy_id2]
lldp [nearest-bridge | nearest-customer | non-tpmr | all] {port *chassis/*slot/port | slot *chassis/*slot | chassis} med network-policy policy_id - [policy_id2]
no lldp {port *chassis/*slot/port | slot *chassis/*slot | chassis} med network-policy policy_id - [policy_id2]
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port**[**-*port2***]** | slot chassis/slot | chassis} tlv management {port-description | system-name | system-description | system-capabilities | management-address} {enable | disable}
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port**[**-*port2***]** | slot chassis/slot | chassis} tlv dot1 {port-vlan | vlan-name} {enable | disable}

lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port [-port2]| slot chassis/slot | chassis} tlv dot3 mac-phy {enable | disable}
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port [-port2] | slot chassis/slot | chassis} tlv med {power | capability} {enable | disable}
lldp {port chassis/slot/port [-port2]| slot chassis/slot | chassis} tlv proprietary {enable | disable}
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port [-port2]| slot chassis/slot | chassis} tlv application {enable | disable}
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2] | slot chassis/slot | chassis} tlv application {fcoe | iscsi | ethertype *etype* | tcp-sctp-port *protocol* | udp-dccp-port *protocol* | port *protocol*} priority *priority*
show lldp system-statistics
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port [-port2] **slot** chassis/slot] statistics
show lldp local-system
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port [-port2]| slot chassis/slot] local-port
show lldp local-management-address
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/]slot/port [-port2] | slot chassis/slot] config [application-tlv]
show lldp network-policy [policy_id]
show lldp [nearest-bridge | nearest-customer | non-tpmr | all] [**slot** chassis/slot| **port** chassis/slot/port] med network-policy
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port [-port2] | slot chassis/slot] remote-system
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port [-port2] | slot chassis/slot] remote-system med {network-policy | inventory}
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port2[-port] | slot chassis/slot] remote-system application-tlv
show lldp agent-destination-address
lldp {chassis/slot/port | chassis/slot | chassis} trust-agent [admin-state] {enable | disable}] [chassis-id-subtype {chassis-component | interface-alias | port-component | mac-address | network-address | interface-name | locally-assigned | any}]
lldp {chassis/slot/port | chassis/slot | chassis} trust-agent violation-action {trap-and-shutdown | trap | shutdown}
show lldp [chassis/slot | *chassis/slot/port*] trusted remote-agent
show lldp [chassis/slot | chassis/slot/port] trust-agent

SIP Commands

sip-snooping admin-state {enable | disable}
sip-snooping {port *chassis/slot/port*[-*port2*] | linkagg *agg_num*} admin-state {enable | disable}
sip-snooping {port *chassis/slot/port*[-*port2*] | linkagg *agg_num*} mode {force-edge | force-non-edge | automatic}
sip-snooping trusted-server [*ip_address1 ip_address2 ip_address ...ip_address8*]
no sip-snooping trusted-server **{***ip_address* | all}
sip-snooping sip-control dscp *num*
sip-snooping sip-control no dscp
sip-snooping sos-call number *string1 string2 … string4*
no sip-snooping sos-call number {*string* | all}
sip-snooping sos-call dscp *num*
sip-snooping udp-port *udp-port1 udp-port 2 ... udp-port 8*
no sip-snooping udp-port {*udp-port* | all}
sip-snooping tcp-port *tcp-port1 tcp-port 2 ... tcp-port 8*
no sip-snooping tcp-port {*tcp-port* | all}
sip-snooping threshold {audio | video | other} {jitter *jitter_ms_num* | packet-lost *% num* | round-trip-delay *round_trip_delay_ms_num* | r-factor *rfactor_num*| mos *mos_num*}
sip-snooping logging-threshold num-of-calls *num*
show sip-snooping call-records {active-calls | ended-calls} [full | threshold-violation]
clear sip-snooping statistics
show sip-snooping config
show sip-snooping ports
show sip-snooping statistics
show sip-snooping registered-clients

Automatic Fabric Commands

auto-fabric admin-state {enable | disable {remove-global-config | remove-vc-reload]}
auto-fabric interface chassis/slot/port[-port2] admin-state {enable | disable}
auto-fabric discovery start
auto-fabric protocols {lacp | mvrp | spb | ip {ospfv2 | ospfv3 | isis | all} | loopback-detection} {interface chassis/slot/port-port2 | chassis} admin-state {enable | disable}
auto-fabric config-save interval seconds
auto-fabric config-save admin-state {enable | disable}
auto-fabric discovery-interval minutes
auto-fabric protocols spb default-profile {single-service | auto-vlan}
auto-fabric protocols spb set-profile {single-service | auto-vlan} interface chassis/*slot/port*[-port2]
show auto-fabric config
show auto-fabric config interface [chassis/slot[-slot2] | chassis/*slot/port*[-port2]]

IP Commands

ip interface {*if_name* | emp | *master emp* | *local chassis-id chassis}* [{address | vip-address} *ip_address*] [mask *subnet_mask*] [admin-state [enable | disable]] [vlan *vlan_id* | service *service_id*] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [e2 | snap] [primary | no primary]
no ip interface *if_name*
ip interface *if_name* address *ip_address/mask* vlan *vlan_id* rtr-port {port *chassis/slot/port* | linkagg *agg_id*} {tagged | untagged}
ip interface *if_name* tunnel [source *ip_address*] [destination *ip_address*] [protocol {ipip | gre}]
ip interface *dhcp-client* [vlan *vlan_id*] [vsi-accept-filter *filter-string* | server-preference] [release | renew] [option-60 opt60_string] [admin {enable | disable}] [local-proxy-arp | no local-proxy-arp]]
no ip interface *dhcp-client*
ip interface dhcp-client no server-preference
ip router primary-address *ip_address*
ip router router-id *ip_address*
ip static-route *ip_address* [mask *mask*] {gateway {gateway_address | null} [tag *num*] [name *string*] | interface *interface_name* | *follows ip_address*} [metric *metric*]
no ip static-route *ip_address* [mask *mask*] [gateway {gateway_address | null} | interface *interface_name* | *follows ip_address*] [metric *metric*]
ip static-route all bfd-state {enable| disable}
ip static-route ipv4_prefix/pfx_length gateway ipv4_host_address bfd-state {enable| disable}
[vrf vrf_name] ip route-pref {static | rip | ospf | isisl2 | isisl1 | ibgp | ebgp | import} *value*
ip default-ttl *hops*
ping {*ip_address* | hostname} [source-interface ip_interface] [count *count*] [size *packet_size*] [interval *seconds*] [timeout *seconds*] [data-pattern string] [dont-fragment] [tos tos_val]
traceroute {*ip_address* | *hostname*} [max-hop *max_hop_count*] [min-hop min_hop_count] [source-interface ip_interface] [probes probe_count] [timeout seconds] [port port_number_value]
[vrf *vrf_name*] ip directed-broadcast {enable | disable}
[vrf *vrf_name*] ip directed-broadcast trusted-source-ip {*ip_address/mask* | *ip_address* mask *subnet_mask*} [destination-ip {*ip_address/mask* | *ip_address* destination-mask *subnet_mask*] | destination-vlan {*vlan_id* | *vlan_id[-vlan_id}*}]
[vrf *vrf_name*] no ip directed-broadcast trusted source-ip *ip_address* {*ip_address/mask* | *ip_address* mask *subnet_mask*}
[vrf *vrf_name*] ip directed-broadcast clear [trusted-source-ip {*ip_address/mask* | *ip_address* mask *subnet_mask*}]
[vrf *vrf_name*] show ip directed-broadcast [trusted-source-ip {*ip_address/mask* | *ip_address* mask *subnet_mask*}] details
[vrf *vrf_name*] ip service {all | *service_name* | port *service_port*} admin-state {enable | disable}
ip service {*service_name*} port {default | *service_port}*
[vrf *vrf_name*] ip service source-ip {Loopback0 | interface_name} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]
[vrf *vrf_name*] no ip service source-ip {Loopback0 | interface_name} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]
[vrf *vrf_name*] ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} {all-routes | route-map *route_map_name*} [admin-state {enable | disable}]
no ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} [all-routes | route-map | *route_map_name*]
ip access-list *access-list-name*
no ip access-list access-list-name
ip access-list *access-list-name* address *address/prefixLen* [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]
no ip access-list access-list-name address address/*prefixLen*
ip route-map *route_map_name* [sequence-number number] action {permit | deny}
no ip route-map *route_map_name* [sequence-number *number*]
ip route-map *route_map_name* [sequence-number *number*] match ip-address **{***access-list-name* **|** ip_address/*prefixLen* [redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]
no ip route-map *route_map_name* [sequence-number *number***]** match ip-address **{***access-list-name* **|** *ip_address/prefixLen* [redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]
ip route-map *route_map_name* [sequence-number *number*] match ipv6-address {*access-list-name* | *ipv6_address/prefixLen* [redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]
no ip route-map *route_map_name* [sequence-number *number*] match ipv6-address *ipv6_address/prefixLen* [redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]
ip route-map *route_map_name* [sequence-number number] match ip-nexthop {*access-list-name* | *ip_address/prefixLen* [permit | deny]}
no ip route-map *route_map_name* [sequence-number *number*] match ip-nexthop {*access-list-name* | *ip_address/prefixLen* [permit | deny]}
ip route-map *route_map_name* [sequence-number *number*] match ipv6-nexthop {*access-list-name* | *ipv6_address/prefixLen* [permit | deny]}
no ip route-map *route_map_name* [sequence-number *number*] match ipv6-nexthop {*access-list-name* | *ipv6_address/prefixLen* [permit | deny]}
ip route-map *route_map_name* [sequence-number *number*] match tag *tag-number*
no ip route-map *route_map_name* [sequence-number *number*] match tag *tag_number*
ip route-map route_map_name [sequence-number number] match ipv4-interface interface_name
no ip route-map route_map_name [sequence-number number] match ipv4-interface interface_name
ip route-map route_map_name [sequence-number number] match ipv6-interface interface_name

no ip route-map route_map_name [sequence-number number] match ipv6-interface interface_name
ip route-map route_map_name [sequence-number number] match metric metric [deviation deviation]
no ip route-map route_map_name [sequence-number number] match metric metric [deviation deviation]
ip route-map *route_map_name* [sequence-number *number*] match route-type {internal | external [type1 | type2] | level1 | level2}
no ip route-map *route_map_name* [sequence-number *number*] match route-type {internal | external [type1 | type2] | level1 | level2}
ip route-map route_map_name [sequence-number number] match protocol {local | static | rip | ospf | isis | bgp}
no ip route-map route_map_name [sequence-number number] match protocol {local | static | rip | ospf | isis | bgp}
ip route-map route_map_name [sequence-number number] match name *string*
no ip route-map route_map_name [sequence-number number] match name *string*
ip route-map *route_map_name* [sequence-number *number*] set metric *metric* [effect {add | subtract | replace | none}]
no ip route-map *route_map_name* [sequence-number *number*] set metric *metric* [effect {add | subtract | replace | none}]
ip route-map *route_map_name* [sequence-number *number*] set metric-type {internal | external [type1 | type2]}
no ip route-map *route_map_name* [sequence-number *number*] set metric-type {internal | external [type1 | type2]}
ip route-map *route_map_name* [sequence-number *number*] set tag *tag_number*
no ip route-map *route_map_name* [sequence-number *number*] set tag *tag_number*
ip route-map *route_map_name* [sequence-number *number*] set community *community_string*
no ip route-map *route_map_name* [sequence-number *number*] set community *community_string*
ip route-map *route_map_name* [sequence-number *number*] set local-preference *value*
no ip route-map *route_map_name* [sequence-number *number*] set local-preference *value*
ip route-map *route_map_name* [sequence-number *number*] set level {level1 | level2 | level1-2}
no ip route-map *route_map_name* [sequence-number *number*] set level {level1 | level2 | level1-2}
ip route-map *route_map_name* [sequence-number *number*] set ip-nexthop *ip_address*
no ip route-map *route_map_name* [sequence-number *number*] set ip-nexthop *ip_address*
ip route-map *route_map_name* [sequence-number *number*] set ipv6-nexthop *ipv6_address*
no ip route-map *route_map_name* [sequence-number *number*] set ipv6-nexthop *ipv6_address*
vrf [create] [*vrf_name* | default] [profile {max | low}]
no vrf *vrf_name*
[vrf vrf_name] ip export {all-routes | route-map route_map_name | to-all-vrfs {all-routes | route-map route_map_name}}
[vrf *vrf_name*] no ip export
[vrf dest_vrf_name] ip import {vrf {src_vrf_name | default} | isid *instance_id*} {all-routes | route-map route_map_name}
[vrf dest_vrf_name] no ip import {vrf {src_vrf_name | default} | isid *instance_id*}
[vrf vrf_name] show ip export
[vrf vrf_name] show ip import
show ip global-route-table [export-vrf vrf_name]
arp *ip_address mac_address* [alias] [arp-name *name*] [interface interface_name] [port chassis/slot/port] [linkagg agg_id]
no arp *ip_address* [alias]
ip distributed-arp admin-state {enable | disable}
clear arp-cache
ip dos arp-poison restricted-address ip_address
no ip dos arp-poison restricted-address ip_address
arp filter *ip_address* [mask *ip_mask*] [*vlan_id*] [sender | target] [allow | block]
no arp filter *ip_address*
clear arp-cache
icmp type *type* code *code* {{enable | disable} | min-pkt-gap *gap*}
icmp unreachable [net-unreachable | host-unreachable | protocol-unreachable | port-unreachable] {{enable | disable} | min-pkt-gap *gap*}
icmp echo [request | reply] {{enable | disable} | min-pkt-gap *gap*}
icmp timestamp [request | reply] {{enable | disable} | min-pkt-gap *gap*}
icmp add-mask [request | reply] {{enable | disable} | min-pkt-gap *gap*}
icmp messages {enable | disable}
ip dos scan close-port-penalty *penalty_value*
ip dos scan tcp open-port-penalty *penalty_value*
ip dos scan udp open-port-penalty *penalty_value*
ip dos scan threshold *threshold_value*
ip dos trap {enable | disable}
ip dos scan decay *decay_value*
ip dos type {port-scan | ping-of-death | land | loopback-src | invalid-ip | invalid-multicast | unicast-ip-mcast-mac | ping-overload | arp-flood | arp-poison} admin-state {enable | disable}
ip tcp half-open-timeout *timeout_value*
show ip traffic
show ip interface [*if_name* | vlan *vlan_id* | dhcp-client]
show ip emp-interfaces
[vrf vrf_name] show ip routes [summary]
[vrf vrf_name] show ip route-pref
[vrf vrf_name] show ipv6 redist [rip | ospf | isis | bgp]
show ip access-list [*access_list_name*]
show ip route-map [*route_map_name*]
[vrf vrf_name] show ip router database [protocol *type* | gateway *ip_address* | dest {*ip_address*/prefixlen | *ip_address*}]
show ip emp-routes

show ip config
show ip protocols
show ip router-id
show ip service
[vrf vrf_name] show ip service source-ip
show ip dos arp-poison
show arp [*ip_address* | *mac_address*]
show ip arp utilization [slot chassis/*slot* | *interfaces*]
show arp filter [*ip_address*]
show icmp control
show icmp [statistics]
show tcp statistics
show tcp ports
show ip tcp half-open-timeout
show udp statistics
show udp ports
show ip dos config
show ip dos statistics
show vrf [*vrf_name* | default]
show vrf-profiles

IPv6 Commands

ipv6 interface if_name [vlan vlan_id | | service *service_id* | tunnel {tunnel_id | 6to4} | loopback0] admin-state [enable | disable]
no ipv6 interface if_name
ipv6 interface *if_name* rtr-port {port *chassis/slot/port* | linkagg *agg_id*} {tagged | untagged} vlan *vlan_id*
ipv6 interface *if_name tunnel {source ipv4_source destination ipv4_destination}*
ipv6 address *ipv6_address /prefix_length* **{***if_name* | *loopback***}**
no ipv6 address *ipv6_address* **{***if_name* | *loopback***}**
ipv6 address *ipv6_prefix* eui-64 **{***if_name* | *loopback***}**
no ipv6 address *ipv6_prefix* eui-64 **{***if_name* | *loopback***}**
ipv6 address global-id {generate | globalID}
ipv6 address local-unicast [global-id globalID] [subnet-id subnetID] {interface-id interfaceID | eui-64} [prefix-length prefixLength] {if_name | loopback}
no ipv6 address local-unicast [global-id globalID] [subnet-id subnetID] {interface-id interfaceID | eui-64} [prefix-length prefixLength] {if_name | loopback}
ipv6 dad-check *ipv6_address if_name*
ipv6 hop-limit *value*
no ipv6 hop-limit
ipv6 pmtu-lifetime *time*
ipv6 neighbor stale-lifetime *stale-lifetime*
ipv6 neighbor *ipv6_address hardware_address* **{***if_name***}** *{port chassis/slot/port* | *linkagg* agg_id*}*
no ipv6 neighbor *ipv6_address* **{***if_name***}**
ipv6 neighbor limit *count*
no ipv6 neighbor limit
ipv6 neighbor vrf-limit *count*
no ipv6 neighbor vrf-limit
ipv6 ra-filter if-name [admin-state {enable | disable}]
no ipv6 ra-filter if-name
ipv6 ra-filter if-name trusted {port chassis/slot/port | linkagg agg_num}
no ipv6 ra-filter if-name trusted {port chassis/slot/port | linkagg agg_num}
ipv6 prefix *ipv6_address /prefix_length if_name [valid-lifetime time] [preferred-lifetime time] [on-link-flag {true | false} [autonomous-flag {true | false}] if_name*
no ipv6 prefix *ipv6_address /prefix_length if_name*
ipv6 static-route *ipv6_prefix/prefix_length* gateway {*ipv6_address* | null} [tag *num*] [name *string*] [*if_name]* [emp] [metric *metric*]
no ipv6 static-route *ipv6_prefix/prefix_length* gateway *{ipv6_address* | null} [*if_name]* [emp]
ipv6 static-route all bfd-state {enable| disable}
ipv6 static-route ipv6_prefix/pfx_length gateway ipv6_host_address bfd-state {enable| disable}
ipv6 route-pref {static | ospf | rip | ebgp | ibgp | isisl1 | isisl2 | import} *value*
ipv6 virtual-source-mac {on | off}
ipv6 echo {anycast | multicast}
no ipv6 echo {anycast | multicast}
ipv6 icmp rate-limit [interval *number*] [burst *number*]
no ipv6 icmp rate-limit
ping6 {*ipv6_address* | *hostname*} *[if_name]* [count *count*] [size *data_size*] [interval *seconds*]
traceroute6 {ipv6_address | hostname} [if_name] [max-hop *hop_count*] [dest-port port_number] [probe-count probe] [size size] [host-names {yes | no}]
modify boot parameters
show ipv6 icmp statistics [if_name]
show ipv6 interface [if_name | loopback]
show ipv6 emp-interface
show ipv6 emp-routes
show ipv6 pmtu table
show ipv6 ra-filter [if-name]
show ipv6 neighbors [ipv6_prefix/prefix_length | if_name | hw hardware_address | static]
clear ipv6 neighbors
show ipv6 prefixes
show ipv6 routes [ipv6_prefix/prefix_length | summary | protocol [bgp| import | isis | local | ospf | rip static]]
show ipv6 route-pref
show ipv6 router database [protocol *type* | gateway *ipv6_address* | dest *ipv6_prefix/ prefix_length*]

show ipv6 tcp connections
show ipv6 tcp listeners
show ipv6 traffic [if_name]
show ipv6 tunnel configured
show ipv6 tunnel 6to4
show ipv6 udp ports
show ipv6 information
ipv6 redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} {all-routes | route-map *route_map_name*} [admin-state {enable | disable}]
ipv6 access-list *access_list_name*
no ipv6 access-list access_list_name
ipv6 access-list *access_list_name* address *address/prefixLen* [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]
no ipv6 access-list access_list_name address address/*prefixLen*
show ipv6 redist [rip | ospf | bgp]
show ipv6 access-list [*access_list_name*]
[vrf vrf_name] ipv6 export {all-routes | route-map route_map_name | to-all-vrfs {all-routes | route-map route_map_name}}
[vrf *vrf_name*] no ipv6 export
[vrf dest_vrf_name] ipv6 import {vrf {src_vrf_name | default} | isid *instance_id*} {all-routes | route-map route_map_name}
[vrf dest_vrf_name] no ipv6 import vrf {src_vrf_name | default}
[vrf vrf_name] show ipv6 export
[vrf vrf_name] show ipv6 import
show ipv6 global-route-table [export-vrf vrf_name]

IPsec Commands

ipsec key *name* {sa-authentication | sa-encryption} [encrypted] *key*
no ipsec key *name* {sa-authentication | sa-encryption}
ipsec security-key [*old_key*] *new_key*
ipsec policy *name* [priority *priority***]** [source **{***ipv6_address***[***/prefix_length***]}** [port *port*]] [destination **{***ipv6_address***[***/prefix_length***]}** [port *port*]] [protocol {any | icmp6 [type t*ype*]| tcp | udp | ospf | vrrp | number *protocol***}**] [in | out] [discard | ipsec | none] [description *description*] [admin-state {enable | disable}]
no ipsec policy *name*
ipsec policy *name* rule *index* [ah | esp]
no ipsec policy *name*
ipsec sa *name* {esp | ah} [source *ipv6_address*] [destination *ipv6_address*] [spi *spi***]** [encryption {null | 3des-cbc | aes-cbc [key-size *key_length*]}] [authentication {none | hmac-md5 | hmac-sha1 | aes-xcbc-mac}] [description *description*] [admin-state {enable | disable}]
no ipsec sa *name*
ipsec default-discard admin-state {enable | disable}
show ipsec policy [name]
show ipsec sa [name | esp | ah]
show ipsec key [sa-encryption | sa-authentication]
show ipsec ipv6 statistics

RIP Commands

ip load rip
ip rip admin-state {enable | disable}
ip rip interface {*interface_name*}
no ip rip interface {*interface_name*}
ip rip interface {*interface_name*} admin-state {enable | disable}
ip rip interface {*interface_name*} metric *value*
ip rip interface {*interface_name*} send-version {none | v1 | v1compatible | v2}
ip rip interface {*interface_name*} recv-version {v1 | v2 | both | none}
ip rip interface {*interface_name*} ingress-filter {*filter_name*}
ip rip interface {*interface_name*} egress-filter {*filter_name*}
ip rip force-holddowntimer *seconds*
ip rip host-route
no ip rip host-route
ip rip route-tag *value*
ip rip interface {*interface_name*} auth-type {none | simple | md5}
ip rip interface {*interface_name*} auth-key *string*
ip rip update-interval *seconds*
ip rip invalid-timer *seconds*
ip rip garbage-timer *seconds*
ip rip holddown-timer *seconds*
show ip rip
show ip rip routes **[***ip_address ip_mask***]**
show ip rip interface **[***interface_name***]**
show ip rip peer [*ip_address*]
ipv6 load rip
ipv6 rip admin-state {enable | disable}
ipv6 rip invalid-timer seconds
ipv6 rip garbage-timer seconds
ipv6 rip holddown-timer seconds
ipv6 rip jitter value
ipv6 rip route-tag value
ipv6 rip update-interval seconds
ipv6 rip triggered-sends {all | updated-only | none}
ipv6 rip interface if_name
no ipv6 rip interface if_name
ipv6 rip interface if_name metric value
ipv6 rip interface if_name recv-status {enable | disable}

ipv6 rip interface if_name send-status {enable | disable}
ipv6 rip interface if_name horizon {none | split-only | poison}
show ipv6 rip
show ipv6 rip interface [if_name]
show ipv6 rip peer [ipv6_addresss]
show ipv6 rip routes [dest ipv6_prefix/prefix_length | gateway ipv6_addr | detail ipv6 prefix/prefix_length]

BFD Commands

ip bfd admin-state {enable | disable}
ip bfd transmit transmit_interval
ip bfd receive receive_interval
ip bfd multiplier num
ip bfd echo-interval echo_interval
{ip | ipv6} bfd interface if_name
no {ip | ipv6} bfd interface if_name
{ip | ipv6} bfd interface if_name admin-state {enable | disable}
{ip | ipv6} bfd interface if_name transmit transmit_interval
{ip | ipv6} bfd interface if_name receive receive_interval
{ip | ipv6} bfd interface if_name multiplier num
{ip | ipv6} bfd interface if_name echo-interval echo_interval
show ip bfd
show {ip | ipv6} bfd interfaces [if_name]
show {ip | ipv6} bfd sessions [session_num] [slot chassis/slot]
show {ip | ipv6} bfd sessions statistics [*session_num*]

DHCP Relay Commands

ip dhcp relay admin-state {enable | disable}
ip dhcp relay destination ip_address
no ip dhcp relay destination ip_address
ip dhcp relay per-interface-mode
no ip dhcp relay per-interface-mode
ip dhcp relay interface if_name destination ip_address
no ip dhcp relay interface if_name destination ip_address
ip dhcp relay interface if_name admin-state {enable | disable}
ip dhcp relay forward-delay *seconds*
ip dhcp relay maximum-hops *hops*
ip dhcp relay insert-agent-information
no ip dhcp relay insert-agent-information
ip dhcp relay insert-agent-information policy {drop | keep | replace}
ip dhcp relay insert-agent-information format {base-mac | system-name | user-string *string* | *interface-alias* | *auto-interface-alias* | *ascii {{circuit-id* | *remoted-id} {base-mac* | *cvlan* | *interface* | *interface-alias* | *system-name* | *user-string string* | *vlan}} {delimiter string}}}
ip dhcp relay pxe-support
no dhcp relay pxe-support
show ip dhcp relay interface
show ip dhcp relay statistics
ip dhcp relay clear statistics [global-only | destination *ip_address* | interface *if_name* destination *ip_address*]
show ip dhcp relay insert-agent-informaton error-count [interface *if_name* | port *chassis/slot/port* [interface *if_name*]]
ip dhcp relay clear insert-agent-informaton error-count [interface *if_name* | port *chassis/slot/port*
show ip dhcp relay counters
ip helper address *ip_address*
no ip helper address [*ip_address*]
ip helper vlan *vlan_id*[-*vlan_id2*] address *ip_address*
no ip helper vlan *vlan_id*[-*vlan_id2*] address *ip_address*
ip helper standard
ip helper per-vlan-only
show ip helper
show ip helper statistics
no ip helper statistics [global-only | server-only | address *ip_address* | vlan *vlan_id* {address *ip_address*}]
ip udp relay port *port_num* [description *description*]
ip udp relay no port *port_num*
ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} [description *description*]
ip udp relay no service {tftp | tacacs | ntp | nbns | nbdd | dns}
ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num* [description *description*]} vlan *vlan_id*[-*vlan_id2*]
ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num*} no vlan *vlan_id*[-*vlan_id2*]}
ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num* [description *description*]} svc *service_id*[-*service_id2*]
ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num*} no svc *service_id*[-*service_id2*]
ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num* [description *description*]} address *ip_address*
ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num*} no address *ip_address*
show ip udp relay [service {tftp | tacacs | ntp | nbns | nbdd | dns} | port *port_num*]
show ip udp relay statistics [service {tftp | tacacs | ntp | nbns | nbdd | dns}] [port [*port_num*]]
ip udp relay no statistics
ipv6 udp relay port *port_num* [description *description*]

ipv6 udp relay no port *port_num*
ipv6 udp relay service {tftp | tacacs | ntp | dns} [description *description*]
ipv6 udp relay no service {tftp | tacacs | ntp | dns}
ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port *port_num* [description *description*]} vlan *vlan_id*[-*vlan_id2*]
ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port *port_num*} no vlan *vlan_id*[-*vlan_id2*]}
ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port *port_num* [description *description*]} svc *service_id*[-*service_id2*]
ipv6 udp relay service {tftp | tacacs | ntp | dns} | port *port_num*} no svc *service_id*[-*service_id2*]
ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port *port_num* [description *description*]} address *ipv6_address*]
ipv6 udp relay service {tftp | tacacs | ntp | dns} | port *port_num* no address *ip6_address*
show ipv6 udp relay [service {tftp | tacacs | ntp | dns} | port *port_num*]
show ipv6 udp relay statistics [service {tftp | tacacs | ntp | dns}] [port [*port_num*]]
ipv6 udp relay clear statistics
ipv6 dhcp relay admin-state {enable | disable}
ipv6 dhcp relay if_name admin-state {enable | disable}
ipv6 dhcp relay if_name destination ip6_address scope_if_name
no ipv6 dhcp relay if_name destination ip6_address scope_if_name
ip dhcp relay maximum-hops *hops*
show ipv6 dhcp relay
dhcp-server {enable | disable}
dhcp-server restart
show dhcp-server leases [ip- address ip_address | mac-address mac_address] [type {static | dynamic}] [count]
show dhcp-server statistics [packets | hosts | subnets | all]
clear dhcp-server statistics
dhcpv6-server {enable | disable}
dhcpv6-server restart
show dhcpv6-server leases [ip- address ipv6_address | type {static | dynamic}] [count]
show dhcpv6-server statistics [packets | hosts | subnets | all]
clear dhcpv6-server statistics
dhcp-message-service {enable | disable}
dhcp-message-service restart
show message-service status
active-lease-service {enable | disable}
active-lease-service restart
show active-lease-service status
dhcp-snooping admin-state {enable | disable}
no dhcp-snooping
dhcp-snooping mac-address-verification admin-state {enable | disable}
dhcp-snooping option-82-data-insertion admin-state {enable | disable}
dhcp-snooping bypass option-82-check admin-state {enable | disable}
dhcp-snooping option-82 format [base-mac | system-name | user-string *string* | *interface-alias* | *auto-interface-alias* | *ascii [{ remote-id* | *circuit-id} {base-mac* | *cvlan* | *interface* | *interface-alias* | *system-name* | *user-string string* | *vlan} {delimiter string}]]*
no dhcp-snooping option-82 format *ascii {remote-id* | *circuit-id}*
dhcp-snooping option-82 policy [replace | keep | drop]
dhcp-snooping vlan *vlan_id*[-*vlan_id2*] [mac-address-verification | option-82-data-insertion] admin-state {enable | disable}
no dhcp-snooping vlan *vlan_id*[-*vlan_id2*]
dhcp-snooping port *chassis*/*slot1*/*port*[-*port2*] {block | client-only | trust}
dhcp-snooping linkagg *agg_id*[-*agg_id2*] {block | client-only | trust}
dhcp-snooping ip-source-filtering admin-state {enable | disable}
dhcp-snooping ip-source-filter {vlan vlan_id[-*vlan_id2*]| port chassis/*slot*/*port*[-*port2*] | linkagg agg_id[-*agg_id2*]} admin-state {enable | disable}
dhcp-snooping binding admin-state {enable | disable}
dhcp-snooping binding timeout *seconds*
dhcp-snooping binding action {purge | renew | save}
dhcp-snooping binding persistency admin-state {enable | disable}
dhcp-snooping binding *mac_address* port chassis/slot/port address ip_address vlan vlan_id
no dhcp-snooping binding mac_address port chassis/slot/port address ip_address vlan vlan_id
show dhcp-snooping
show dhcp-snooping ip-source-filter {vlan | port}
show dhcp-snooping vlan
show dhcp-snooping port
dhcp-snooping clear violation-counters {port chassis/*slot*/*port* [-*port2*]} | slot chassis/*slot* | linkagg agg_id | all}
show dhcp-snooping counters [slot *chassis_id*/*slot_id*]
dhcp-snooping clear counters
show dhcp-snooping isf-statistics [vlan *vlan_id*]
dhcp-snooping clear isf-statistics
show dhcp-snooping binding [port chassis/*slot*/*port*] | linkagg agg_id | ip-address *ip_address* | snapshot [static | dynamic]]
dhcpv6-snooping vlan *vlan_id*[-*vlan_id2*] admin-state {enable | disable}
no dhcpv6-snooping vlan *vlan_id*[-*vlan_id2*]
dhcpv6-snooping global admin-state {enable | disable}
dhcpv6-snooping binding vlan *vlan_id* link-local *ipv6_address* [global-address *ipv6_address*] [mac-address *mac_address*] [port *chassis/slot/port* | linkagg *agg_id*]
no dhcpv6-snooping binding vlan *vlan_id* link-local *ipv6_address*
dhcpv6-snooping binding timeout *seconds*
dhcpv6-snooping binding action {purge | renew | save}
dhcpv6-snooping binding persistency {enable | disable}
dhcpv6-snooping ipv6-source-filter {vlan *vlan_id*[-*vlan_id2*] | port *chassis/slot1/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} admin-state {enable | disable}
ipv6 dhcp guard vlan vlan_id [client {enable | disable}] [admin-state {enable | disable}]
no ipv6 dhcp guard vlan vlan_id

ipv6 dhcp guard vlan vlan_id trusted [port *chassis/slot/port* | linkagg *agg_id*]
no ipv6 dhcp guard vlan vlan_id trusted [port *chassis/slot/port* | linkagg *agg_id*]
show dhcpv6-snooping
show dhcpv6-snooping interfaces
show dhcpv6-snooping binding [global-address *ipv6_address*] [port *chassis/slot/port* | linkagg *agg_id*]
show dhcpv6-snooping ipv6-source-filter
show ipv6 dhcp guard [vlan vlan_id]

VRRP Commands

{ip | ipv6} vrrp *vrid* interface *if_name* admin-state **[**enable | disable] [priority *priority*] [preempt | no preempt] [accept | no accept] [interval *centiseconds*] [version {v2 | v3}
no {ip | ipv6} *vrid* interface *if_name*
{ip | ipv6} vrrp *vrid* interface *if_name* address {*ipv4_address* | *ipv6_address*}
{ip | ipv6} vrrp *vrid* interface *if_name* no address {*ipv4_address* | *ipv6_address*}
ip vrrp track *track_id* [admin-state [enable | disable] | priority *priority* | ipv4-interface *if_name* | ipv6-interface *if_name* | port *chassis/slot/port* | address *ip_address* [bfd-state {enable | disable} | delay *seconds*]**]**
no ip vrrp track *track_id*
ip vrrp bfd-state {enable | disable}
{ip | ipv6} vrrp *vrid* interface *if_name* track-association *track_id*
{ip | ipv6} vrrp *vrid* interface *if_name* no track-association *track_id*
ip vrrp delay *seconds*
ip vrrp version [v2 | v3]
{ip | ipv6} vrrp interval *centiseconds*
{ip | ipv6} vrrp priority *priority*
{ip | ipv6} vrrp [preempt | no preempt]
{ip | ipv6} vrrp [accept | no accept]
{ip | ipv6} vrrp admin-state [disable | enable | enable-all]
{ip | ipv6} vrrp set {interval | priority | preempt | accept | version | all | none} [override]
{ip | ipv6} vrrp group *vrgid* [interval *centiseconds***]** [priority *priority*] [preempt | no preempt] [accept | no accept] [version {v2 | v3}
{ip | ipv6} vrrp group *vrgid* admin-state [disable | enable | enable-all]
{ip | ipv6} vrrp group *vrgid* set [interval | priority | preempt | accept | version | all] [override]
{ip | ipv6} vrrp *vrid* interface *if_name* group-association *vrgid*
show {ip | ipv6} vrrp [*vrid*]
show {ip | ipv6} [*vrid*] statistics
show ip vrrp track [*track_id*]
show {ip | ipv6} [*vrid*] track-association [*track_id*]
show {ip | ipv6} vrrp group **[***vrgid***]**
show {ip | ipv6} vrrp group-association **[***vrgid***]**

OSPF Commands

ip load ospf
ip ospf admin-state {enable | disable}
ip ospf asbr
no ip ospf asbr
ip ospf exit-overflow-interval *seconds*
ip ospf extlsdb-limit *limit*
ip ospf host *ip_address* tos *tos* [metric *metric*]
no ip ospf host *ip_address* tos *tos*
ip ospf mtu-checking
no ip ospf mtu-checking
ip ospf default-originate {only | always} [metric-type {type1 | type2}] [metric *value*]
no ip ospf default-originate
ip ospf route-tag *tag*
ip ospf spf-timer [delay *delay_seconds*] [hold *hold_seconds*]
ip ospf virtual-link *area_id router_id* [auth-type {none | simple | md5}] [auth-key *key_string*] [dead-interval *seconds*] [hello-interval *seconds*] [retrans-interval *seconds*] [transit-delay *seconds*]
no ip ospf virtual-link *area_id router_id*
ip ospf neighbor *neighbor_id* {eligible | ineligible}
no ip ospf neighbor *neighbor_id*
ip ospf area *area_id* [summary {enable | disable}] | [type {normal | stub | nssa}]
no ip ospf area *area_id*
ip ospf area *area_id* default-metric *tos* **[**[cost *cost*] | [type {ospf | type 1 | type 2}]
no ip ospf area *area_id* default-metric *tos*
ip ospf area *area_id* range {summary | nssa} *ip_address subnet_mask* [effect {admatching | noMatching}]
no ip ospf area *area_id* range {summary | nssa} *ip_address subnet_mask*
ip ospf interface {*interface_name*}
no ip ospf interface {*interface_name*}
ip ospf interface {*interface_name*} admin-state {enable | disable}
no ip ospf interface {*interface_name*} admin-state {enable | disable}
ip ospf interface {*interface_name*} area *area_id*
ip ospf interface {*interface_name*} auth-key *key_string*
ip ospf interface {*interface_name*} auth-type {none | simple | md5 | key-chain *key-chain-id*}
ip ospf interface {*interface_name*} dead-interval *seconds*
ip ospf interface {*interface_name*} hello-interval *seconds*
ip ospf interface {*interface_name*} md5 *key_id* [enable | disable]
ip ospf interface {*interface_name*} md5 *key_id* key *key_string*
ip ospf interface {*interface_name*} type {point-to-point | point-to-multipoint | broadcast | non-broadcast}
ip ospf interface {*interface_name*} cost *cost*
ip ospf interface {*interface_name*} poll-interval *seconds*

ip ospf interface {*interface_name*} priority *priority*
ip ospf interface {*interface_name*} retrans-interval *seconds*
ip ospf interface {*interface_name*} transit-delay *seconds*
ip ospf bfd-state {enable | disable}
ip ospf bfd-state all-interfaces {enable | disable}
ip ospf interface *if_name* bfd-state {enable | disable}
ip ospf interface *if_name* bfd-state drs-only
ip ospf interface *if_name* bfd-state all-neighbors {enable | disable}
ip ospf restart-support {planned-unplanned | planned-only}
no ip ospf restart-support
ip ospf restart-interval [*seconds*]
ip ospf restart-helper [admin-state {enable | disable}]
ip ospf restart-helper strict-lsa-checking admin-state {enable | disable}
ip ospf restart initiate
show ip ospf
show ip ospf border-routers [*area_id*] [*router_id*] [*tos*] [*gateway*]
show ip ospf ext-lsdb [linkstate-id *ls_id*] [router-id *router_id*]
show ip ospf host [*ip_address*]
show ip ospf lsdb [*area_id*] [rtr | net | netsum | asbrsum] [linkstate-id *ls_id*] [router-id *router_id*]
show ip ospf neighbor [*ip_address*]
show ip ospf routes [ip_address *mask tos gateway*]
show ip ospf virtual-link [*router_id*]
show ip ospf virtual-neighbor *area_id router_id*
show ip ospf area [*area_id*]
show ip ospf area *area_id* range [{summary | nssa} *ip_address ip_mask*]
show ip ospf area *area_id* stub
show ip ospf interface [*interface_name*]
show ip ospf interface auth-info [*interface_name*]
show ip ospf restart

OSPFv3 Commands

ipv6 load ospf
ipv6 ospf admin-state {enable | disable}
ipv6 ospf host *ipv6_address* [*area area_id*] [metric *metric*]
no ipv6 ospf host *ipv6_address area area_id*
ipv6 ospf mtu-checking
no ipv6 ospf mtu-checking
ipv6 ospf route-tag *tag*
ipv6 ospf spf-timer [delay *delay_seconds*] [hold *hold_seconds*]
ipv6 ospf virtual-link area *area_id* router *router_id* [dead-interval *seconds*] [hello-interval *seconds*] [retrans-interval *seconds*] [transit-delay *seconds*]
no ipv6 ospf virtual-link area *area_id* router *router_id*
ipv6 ospf area *area_id* [type {normal | stub [default-metric *metric*] | nssa [default-metric *metric*]}] | [summarize [filter]
no ipv6 ospf area *area_id*
ipv6 ospf area *area_id* [area-summary {noareasummary | sendareasummary}]
ipv6 ospf area *area_id* [nssa-translator-role {always | candidate}]
ipv6 ospf area *area_id* [nssa-translator-stab-interval *interval*]
ipv6 ospf area *area_id* nssa-summarize *ipv6_address_prefix* [filter]
ipv6 ospf interface *interface_name*
no ipv6 ospf interface *interface_name*
ipv6 ospf interface *interface_name* admin-state {enable | disable}
no ipv6 ospf interface *interface_name*
ipv6 ospf interface *interface_name suppress-link-lsa*
no ipv6 ospf interface *interface_name suppress-link-lsa*
ipv6 ospf interface *interface_name* type {broadcast | point-to-point | point-to-multipoint | nbma}
ipv6 ospf neighbor *nbr_ipv6_address* interface *interface_name* {eligible | ineligible}
no ipv6 ospf neighbor *nbr_ipv6_address*
ipv6 ospf interface *interface_name* area *area_id*
ipv6 ospf interface *interface_name* dead-interval *seconds*
ipv6 ospf interface *interface_name* hello-interval *seconds*
ipv6 ospf interface *interface_name* cost *cost*
ip ospf interface *interface_name* priority *priority*
ipv6 ospf interface *interface_name* retrans-interval *interval*
ipv6 ospf interface *interface_name* transit-delay *delay*
ipv6 ospf bfd-state {enable | disable}
ipv6 ospf bfd-state all-interfaces {enable | disable}
ipv6 ospf interface *if_name* bfd-state {enable | disable}
ipv6 ospf interface *if_name* bfd-state drs-only
ipv6 ospf interface *if_name* bfd-state all-neighbors {enable | disable}
show ipv6 ospf
show ipv6 ospf border-routers [area *area_id*] [router *router_id*]
show ipv6 ospf host [*ipv6_address*]
show ipv6 ospf lsdb [area *area_id*] [rtr | net | netsum | asbrsum] [linkstate-id *ls_id*] [router-id *router_id*]
show ipv6 ospf neighbor [router *ipv4_address*][interface *interface_name*]
show ipv6 ospf routes [prefix ipv6_address_prefix][gateway gateway]
show ipv6 ospf virtual-link [*router_id*]
show ipv6 ospf area [*area_id*]
show ipv6 ospf interface [*interface_name*]
ipv6 ospf restart
ipv6 ospf restart initiate
ipv6 ospf restart interval [*seconds*]
ipv6 ospf restart-helper

ipv6 ospf restart-helper strict-lsa-check
show ipv6 ospf restart

IS-IS Commands

ip load isis
ip isis admin-state {enable | disable}
ip isis area-id *area address*
no ip isis area-id *area address*
ip isis level-capability {level-1 | level-2 | level-1/2}
ip isis auth-check {enable | disable}
ip isis auth-type {simple {key *key* | encrypt-key *encrypt_key*} | md5 {key *key* | encrypt-key *encrypt_key*} | key-chain *key-chain-id* | none}
ip isis csnp-auth
no ip isis csnp-auth
ip isis hello-auth
no ip isis hello-auth
ip isis psnp-auth
no ip isis psnp-auth
ip isis lsp-lifetime *seconds*
no ip isis lsp-lifetime
ip isis lsp-wait {max-wait | initial-wait | second-wait} *seconds*
no ip isis lsp-wait {max-wait | initial-wait | second-wait}
ip isis spf-wait {max-wait *seconds* | initial-wait *milliseconds*| second-wait *milliseconds*}
no ip isis spf-wait {max-wait | initial-wait | second-wait}
ip isis summary-address {*ip_prefix/mask* | *ip_prefix* [/*netmask*]} {level-1 | level-2 | level-1/2}
no ip isis summary-address {*ip_prefix/mask* | *ip_prefix* [/*netmask*]}
ip isis overload [timeout *seconds*]
no ip isis overload [timeout]
ip isis overload-on-boot [timeout *seconds*]
no ip isis overload-on-boot [timeout *seconds*]
ip isis graceful-restart
no ip isis graceful-restart
ip isis graceful-restart helper {enable | disable}
ip isis strict-adjacency-check {enable | disable}
ip isis level {1 | 2} auth-type {simple {key *key* | *encrypt-key encrypt_key*} | md5 {key *key* | *encrypt-key encrypt_key*} | key-chain *key-chain-id* | none}
ip isis level {1 | 2} hello-auth
no ip isis level {1 | 2} hello-auth
ip isis level {1 | 2} csnp-auth
no ip isis level {1 | 2} csnp-auth
ip isis level {1 | 2} psnp-auth
no ip isis level {1 | 2} psnp-auth
ip isis level {1 | 2} wide-metrics-only
no ip isis level {1 | 2} wide-metrics-only
ip isis {activate-ipv6 | activate-ipv4}
no ip isis {activate-ipv6 | activate-ipv4}
ip isis vlan vlan_id [address-family {v4 | v6 | v4v6}]
ip isis vlan vlan_id admin-state {enable | disable}
ip isis vlan vlan_id interface-type {broadcast | point-to-point}
ip isis vlan vlan_id csnp-interval seconds
ip isis vlan vlan_id hello-auth-type {simple {key key | encrypt-key encrypt_key} | md5 {key key | encrypt-key encrypt_key} | key-chain *key-chain-id* | none}
ip isis vlan vlan_id level-capability [level-1 | level-2 | level-1/2]
ip isis vlan vlan_id lsp-pacing-interval *milliseconds*
no ip isis vlan vlan_id lsp-pacing-interval
ip isis vlan vlan_id passive
no ip isis vlan vlan_id passive
ip isis vlan vlan_id retransmit-interval *seconds*
no ip isis vlan vlan_id retransmit-interval
ip isis vlan vlan_id default-type
ip isis vlan vlan_id level {1 | 2} hello-auth-type {simple {key *key* | encrypt-key *encrypt_key*} | md5 {key *key* | encrypt-key *encrypt_key*} | key-chain *key-chain-id* | none}
ip isis vlan vlan_id level {1 | 2} hello-interval *seconds*
no ip isis vlan vlan_id level {1 | 2} hello-interval
ip isis vlan vlan_id level {1 | 2} hello-multiplier *number*
no ip isis vlan vlan_id level {1 | 2} hello-multiplier
ip isis vlan vlan_id level {1 | 2} metric *number*
no ip isis vlan vlan_id level {1 | 2} metric
ip isis vlan vlan_id level {1 | 2} passive
no ip isis vlan vlan_id level {1 | 2} passive
ip isis vlan vlan_id level [1 | 2] priority *number*
no ip isis vlan vlan_id level [1 | 2] priority
ip isis summary-address6 {ipv6_prefix/prefix_length | ipv6_address} {level-1 | level-2 | level-1/2}
no ip isis summary-address6 {ipv6_prefix/prefix_length | ipv6_address} {level-1 | level-2 | level-1/2}
ip isis bfd-state {enable | disable}
ip isis bfd-state all-vlans {enable | disable}
ip isis vlan vlan_id bfd-state {enable | disable}
show ip isis adjacency [{system-id *nbr_sys_id* | vlan *vlan_id*}] [detail]
show ip isis database [{system_id *system_id* | lsp_id *lsp_id*}] [detail] [level {1 | 2}]
show ip isis hostname
show ip isis routes
show ip isis routes6
show ip isis spf [detail]
show ip isis spf-log [detail]
show ip isis statistics

show ip isis status
show ip isis summary-address [*ip_address* [/*mask*]]
show ip isis vlan [vlan_id] [detail]
show ip isis summary-address6 [*ip_address* [/*mask*]]
clear ip isis adjacency [system-id *nbr_sys_id*]
clear ip isis lsp-database [system-id *sys_id*]
clear ip isis spf-log
clear ip isis statistics
ip isis multi-topology
no ip isis multi-topology

BGP Commands

ip load bgp
ip bgp admin-state {enable | disable}
ip bgp autonomous-system *value*
ip bgp bestpath as-path ignore
no ip bgp bestpath as-path ignore
ip bgp cluster-id *ip_address*
ip bgp default local-preference *value*
ip bgp fast-external-failover
no ip bgp fast-external-failover
ip bgp always-compare-med
no ip bgp always-compare-med
ip bgp bestpath med missing-as-worst
no ip bgp bestpath med missing-as-worst
ip bgp client-to-client reflection
no ip bgp client-to-client reflection
ip bgp as-origin-interval *seconds*
no ip bgp as-origin-interval
ip bgp synchronization
no ip bgp synchronization
ip bgp confederation identifier *value*
ip bgp maximum-paths
no ip bgp maximum-paths
ip bgp log-neighbor-changes
no ip bgp log-neighbor-changes
ip bgp dampening [half-life *half_life* reuse *reuse* suppress *suppress* max-suppress-time *max_suppress_time*]
no ip bgp dampening
ip bgp dampening clear
ip bgp asn-format {asdot | asplain}
ip bgp aggregate-address *ip_address ip_mask*
no ip bgp aggregate-address *ip_address ip_mask*
ip bgp aggregate-address *ip_address ip_mask* admin-state {enable | disable}
ip bgp aggregate-address *ip_address ip_mask* as-set
no ip bgp aggregate-address *ip_address ip_mask* as-set
ip bgp aggregate-address *ip_address ip_mask* community {none | no-export | no-advertise | no-export-subconfed | *num:num*}
ip bgp aggregate-address *ip_address ip_mask* local-preference *value*
no ip bgp aggregate-address *ip_address ip_mask* local-preference *value*
ip bgp aggregate-address *ip_address ip_mask* metric *value*
no ip bgp aggregate-address *ip_address ip_mask* metric *value*
ip bgp aggregate-address *ip_address ip_mask* summary-only
no ip bgp aggregate-address *ip_address ip_mask* summary-only
ip bgp network ip_address *ip_mask*
no ip bgp network ip_address ip_mask
ip bgp network ip_address *ip_mask* admin-state {enable | disable}
ip bgp network *ip_address ip_mask* community {none | no-export | no-advertise | no-export-subconfed | *num:num*}
ip bgp network *ip_address ip_mask* local-preference *value*
no ip bgp network *ip_address ip_mask* local-preference *value*
ip bgp network *ip_address ip_mask* metric *value*
no ip bgp network *ip_address ip_mask* metric *value*
ip bgp neighbor *ip_address*
no ip bgp neighbor *ip_address*
ip bgp neighbor *ip_address* ttl-security *num*
ip bgp neighbor *ip_address* no ttl-security
ip bgp neighbor *ip_address* [activate-ipv4]
no ip bgp neighbor i*p_address* [activate-ipv4]
ip bgp neighbor *ip_address* admin-state {enable | disable}
ip bgp neighbor *ip_address* advertisement-interval *value*
ip bgp neighbor *ip_address* clear
ip bgp neighbor *ip_address* route-reflector-client
no ip bgp neighbor *ip_address* route-reflector-client
ip bgp neighbor *ip_address* default-originate
no ip bgp neighbor *ip_address* default-originate
ip bgp neighbor *ip_address* timers *keepalive holdtime*
ip bgp neighbor *ip_address* conn-retry-interval *seconds*
ip bgp neighbor *ip_address* auto-restart
ip bgp neighbor *ip_address* maximum-prefix *maximum* [warning-only]
ip bgp neighbor *ip_address* md5 key {*string* | none}
ip bgp neighbor *ip_address* ebgp-multihop [*ttl*]
no ip bgp neighbor *ip_address* ebgp-multihop
ip bgp neighbor *ip_address* description *string*
ip bgp neighbor *ip_address* next-hop-self
no ip bgp neighbor *ip_address* next-hop-self
ip bgp neighbor *ip_address* passive

no ip bgp neighbor *ip_address* passive
ip bgp neighbor *ip_address* remote-as *value*
ip bgp neighbor *ip_address* remove-private-as
no ip bgp neighbor *ip_address* remove-private-as
ip bgp neighbor *ip_address* soft-reconfiguration
no ip bgp neighbor *ip_address* soft-reconfiguration
ip bgp neighbor *ip_address* stats-clear
ip bgp confederation neighbor *ip_address*
no ip bgp confederation neighbor *ip_address*
ip bgp neighbor *ip_address* update-source [*interface_name*]
ip bgp neighbor *ip_address* in-aspathlist {*string* | none}
ip bgp neighbor *ip_address* in-communitylist {*string* | none}
ip bgp neighbor *ip_address* in-prefixlist {*string* | none}
ip bgp neighbor *ip_address* in-prefix6list {*string* | none}
ip bgp neighbor *ip_address* out-aspathlist {*string* | none}
ip bgp neighbor *ip_address* out-communitylist {*string* | none}
ip bgp neighbor *ip_address* out-prefixlist {*string* | none}
ip bgp neighbor *ip_address* out-prefix6list {*string* | none}
ip bgp neighbor *ip_address* route-map {*string* | none} {in | out}
no ip bgp neighbor *ip_address* route-map {in | out}
ip bgp neighbor *ip_address* clear soft {in | out}
ip bgp bfd-state {enable | disable}
ip bgp bfd-state all-neighbors {enable | disable}
{ip | ipv6} bgp neighbor **{**ipv4_address | ipv6_address**}** bfd-state {enable | disable}
ip bgp policy aspath-list *name* "*regular_expression*"
no ip bgp policy aspath-list *name* "*regular_expression*"
ip bgp policy aspath-list *name* **"***regular_expression***"** action {permit | deny}
ip bgp policy aspath-list *name* "*regular_expression*" priority *value*
ip bgp policy community-list *name* {*num:num* | *num.num:num* | *num*}
no ip bgp policy community-list *name* {*num:num* | *num.num:num* | *num*}
ip bgp policy community-list *name* {none | no-export | no-advertise | no-export-subconfed | *num:num*} action {permit | deny}
ip bgp policy community-list *name* {none | no-export | no-advertise | no-export-subconfed | *num:*num}
match-type {exact | occur}
ip bgp policy community-list *name* {none | no-export | no-advertise | no-export-subconfed | *num:num*} priority *value*
ip bgp policy prefix-list *name ip_address ip_mask*
no ip bgp policy prefix-list *name ip_address ip_mask*
ip bgp policy prefix-list *name ip_address ip_mask* action {permit | deny}
ip bgp policy prefix-list *name ip_address ip_mask* ge *value*
ip bgp policy prefix-list *name ip_address ip_mask* le *value*
ip bgp policy prefix6-list *pfx_list_name prefix6/pfx_length [action {permit | deny}] [admin-state {enable | disable}] [ge [{masklength}]] [le [{masklength}]]*
no ip bgp policy prefix6-list *pfx_list_name prefix6/pfx_length [action {permit | deny}] [admin-state {enable | disable}] [ge [{*mask_length*}]] [le [{*mask_length*}]]*
ip bgp policy route-map *name sequence_number*
ip bgp policy route-map *name sequence_number* action {permit | deny}
ip bgp policy route-map *name sequence_number* aspath-list *as_name*
ip bgp policy route-map *name sequence_number* asprepend *path*
ip bgp policy route-map *name sequence_number* community [none | no-export | no-advertise | no-export-subconfed | *num*:*num*]
ip bgp policy route-map *name sequence_number* community-list [*list_name* | none]
ip bgp policy route-map *name sequence_number* community-mode {add | replace}
ip bgp policy route-map *name sequence_number* lpref *value*
ip bgp policy route-map *name sequence_number* lpref-mode {none | inc | dec | rep}
ip bgp policy route-map *name sequence_number* match-community [none | no-export | no-advertise | no-export-subconfed | *num:num*]
ip bgp policy route-map *name sequence_number* match-mask *ip_address*
ip bgp policy route-map *name sequence_number* match-prefix *ip_address*
ip bgp policy route-map *name sequence_number* match-prefix6 *ipv6_address/mask_length*
ip bgp policy route-map *name sequence_number* match-regexp "*regular_expression*"
ip bgp policy route-map *name sequence_number* med *value*
ip bgp policy route-map *name sequence_number* med-mode {none | inc | dec | rep}
ip bgp policy route-map *name sequence_number* origin {igp | egp| incomplete | none}
ip bgp policy route-map *name sequence_number* prefix-list *prefix_name*
ip bgp policy route-map *name sequence_number* prefix6-list *prefix6_name*
ip bgp policy route-map *name sequence_number* weight *value*
ip bgp policy route-map *name sequence_number* community-strip *community_list*
show ip bgp
show ip bgp statistics
show ip bgp dampening
show ip bgp dampening-stats [*ip_address ip_mask] [peer_address*]
show ip bgp path
show ip bgp routes [*ip_address ip_mask*]
show ip bgp aggregate-address [*ip_address ip mask*]
show ip bgp network [*ip_address ip_mask*]
show ip bgp neighbors [*ip_address*]
show ip bgp neighbors policy [*ip_address*]
show ip bgp neighbors timer [*ip_address*]
show ip bgp neighbors statistics [*ip_address*]
show ip bgp policy aspath-list [*name*] [*"regular_expression"*]
show ip bgp policy community-list [*name*] [*string*]
show ip bgp policy prefix-list [*name*] [*ip_address ip_mask*]
show ip bgp policy prefix6-list [*name*] [ipv6_address/prefixLength]
show ip bgp policy route-map [*name*] [*sequence_number*]
ip bgp graceful-restart
no ip bgp graceful-restart

ip bgp graceful-restart restart-interval [*seconds*]
ip bgp unicast
no ip bgp unicast
ipv6 bgp unicast
no ipv6 bgp unicast
ip bgp neighbor *ip_address* activate-ipv6
no ip bgp neighbor i*p_address* activate-ipv6
ip bgp neighbor *ip_address* ipv6-nexthop *ipv6_address*
show ipv6 bgp path [ipv6-addr *ipv6_address/prefix_length*] [detail]
show ipv6 bgp routes
ipv6 bgp network *ipv6_address/prefix_length*
no ipv6 bgp network *ipv6_address/prefix_length*
ipv6 bgp network *ipv6_address/prefix_length* [community {none | no-export | no-advertise | no-export-subconfed | *num* | *num:num*}]
ipv6 bgp network *ipv6_address/prefix_length* **[**local-preference num]
ipv6 bgp network *ipv6_address/prefix_length* **[**metric num]
ipv6 bgp network *ipv6_address/prefix_length* [admin-state **{**enable | disable}]
show ipv6 bgp network **[***ipv6_address/prefix_length***]**
ipv6 bgp neighbor *ipv6_address*
no ipv6 bgp neighbor *ipv6_address*
ipv6 bgp neighbor *ipv6_address ttl-security num*
ipv6 bgp neighbor *ipv6_address* no ttl-security
ipv6 bgp neighbor *ipv6_address* [activate-ipv4]
no ipv6 bgp neighbor i*pv6_address* [activate-ipv4]
ipv6 bgp neighbor *ipv6_address* [activate-ipv6]
no ipv6 bgp neighbor i*pv6_address* [activate-ipv6]
ipv6 bgp neighbor *ipv6_address* [ipv6-nexthop *ipv6_address***]**
ipv6 bgp neighbor *ipv6_address* [admin-state {enable | disable}]
ipv6 bgp neighbor ipv6_address clear
ipv6 bgp neighbor *ipv6_address* auto-restart
ipv6 bgp neighbor *ipv6_address* [remote-as *value***]**
ipv6 bgp neighbor *ipv6_address* [timers *num num*]
ipv6 bgp neighbor *ipv6_address* [maximum-prefix *num* [warning-only]]
no ipv6 bgp neighbor *ipv6_address* [maximum-prefix *num* [warning-only]]
ipv6 bgp neighbor *ipv6_address* [next-hop-self]
no ipv6 bgp neighbor *ipv6_address* [next-hop-self]
ipv6 bgp neighbor *ipv6_address* [conn-retry-interval *num***]**
ipv6 bgp neighbor *ipv6_address* [default-originate]
no ipv6 bgp neighbor *ipv6_address* [default-originate]
ipv6 bgp neighbor *ipv6_address* [update-source *interface_name***]**
no ipv6 bgp neighbor *ipv6_address* [update-source *interface_name***]**
ipv6 bgp neighbor *ipv6_address* [ipv4-nexthop *ip_address***]**
ipv6 bgp neighbor *ipv6_address* advertisement-interval *value*
ipv6 bgp neighbor *ipv6_address* description *string*
ipv6 bgp neighbor *ipv6_address* ebgp-multihop [*ttl*]
no ipv6 bgp neighbor *ipv6_address* ebgp-multihop
ipv6 bgp neighbor *ipv6_address* update-source-address *ipv6_address*
no ipv6 bgp neighbor *ipv6_address* update-source-address *ipv6_address*
ipv6 bgp neighbor *ipv6_address* passive
no ipv6 bgp neighbor *ipv6_address* passive
ipv6 bgp neighbor *ipv6_address* remove-private-as
no ipv6 bgp neighbor *ipv6_address* remove-private-as
ipv6 bgp neighbor *ipv6_address* soft-reconfiguration
no ipv6 bgp neighbor *ipv6_address* soft-reconfiguration
ipv6 bgp neighbor *ipv6_address* stats-clear
ip bgp confederation neighbor6 *ipv6_address*
no ip bgp confederation neighbor6 *ipv6_address*
ipv6 bgp neighbor *ipv6_address* in-aspathlist {*string* | none}
ipv6 bgp neighbor *ipv6_address* in-communitylist {*string* | none}
ipv6 bgp neighbor *ipv6_address* in-prefixlist {*string* | none}
ipv6 bgp neighbor *ipv6_address* in-prefix6list {*string* | none}
ipv6 bgp neighbor *ipv6_address* out-aspathlist {*string* | none}
ipv6 bgp neighbor *ipv6_address* out-communitylist {*string* | none}
ipv6 bgp neighbor *ipv6_address* out-prefixlist {*string* | none}
ipv6 bgp neighbor *ipv6_address* out-prefix6list {*string* | none}
ipv6 bgp neighbor *ipv6_address* route-map {*string* | none} {in | out}
no ipv6 bgp neighbor *ipv6_address* route-map {in | out}
ipv6 bgp neighbor *ipv6_address* clear soft {in | out}
ipv6 bgp neighbor *ipv6_address* route-reflector-client
no ipv6 bgp neighbor *ipv6_address* route-reflector-client
ipv6 bgp neighbor *ipv6_address* md5 key {*string* | none}
show ipv6 bgp neighbors [*ipv6_address*]
show ipv6 bgp neighbors statistics [*ipv6_address*]
show ipv6 bgp neighbors policy *ipv6_address*
show ipv6 bgp neighbors timers [*ipv6_address*]

Server Load Balancing Commands

ip slb admin-state {enable | disable}
ip slb reset statistics
ip slb cluster name {vip ip_address | condition string} [l3 | l2]
no ip slb cluster name
ip slb cluster cluster_name admin-state {enable | disable}
ip slb cluster cluster_name ping period seconds
ip slb cluster *cluster_name* ping timeout *milliseconds*
ip slb cluster *cluster_name* ping retries *count*
ip slb cluster cluster_name probe *probe_name*

ip slb server ip *ip_address* cluster *cluster_name* [admin-state {enable | disable}] [weight *weight]*
no ip slb server ip *ip_address* cluster *cluster_name*
ip slb server ip *ip_address* cluster *cluster_name* probe *probe_name*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
no ip slb probe *probe_name*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} timeout *seconds*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} period *seconds*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} port *port_number*
ip slb probe *probe_name* {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} retries *retries*
ip slb probe *probe_name* {http | https} username *user_name*
ip slb probe *probe_name* {http | https} password *password*
ip slb probe *probe_name* {http | https} url *url*
ip slb probe *probe_name* {http | https} status *status_value*
ip slb probe *probe_name* {tcp | udp} send *send_string*
ip slb probe *probe_name* {http | https | tcp | udp} expect *expect_string*
show ip slb
show ip slb clusters [statistics]
show ip slb cluster *name* [statistics]
show ip slb cluster *name* server *ip_address*
show ip slb servers
show ip slb probes [*probe_name*]

IP Multicast Switching Commands

ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] admin-state [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] admin-state
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** flood-unknown [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** flood-unknown
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] version [*version*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] version
ip multicast {port *chassis/slot/port* **|** sap port *sap_id*} max-group [*num*] [action {none | drop | replace}]
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** max-group [num] [action {none | drop | replace}]
ip multicast static-neighbor vlan *vlan_id* {port *chassis/slot/port* | *linkagg agg_id}*
ip multicast static-neighbor service *service_id* sap {port | *linkagg} {sap_id*}
no ip multicast static-neighbor vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
no ip multicast static-neighbor service *service_id* sap {port | *linkagg} {sap_id*}
ip multicast static-querier vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
ip multicast static-querier service *service_id* sap {port | *linkagg} {sap_id*}
no ip multicast static-querier vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
no ip multicast static-querier service *service_id* sap {port | *linkagg} {sap_id*}
ip multicast static-group *ip_address* vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
ip multicast static-group *ip_address* service *service_id* sap {port | *linkagg} {sap_id*}
no ip multicast static-group *ip_address* vlan *vlan_id* {port *chassis/slot/port* | linkagg *agg_id*}
no ip multicast static-group *ip_address* service *service_id* sap {port | *linkagg} {sap_id*}
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*] query-interval [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*] query-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** last-member-query-interval [tenths_of_seconds**]**
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** last-member-query-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*] query-response-interval [tenths_of_seconds]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*] query-response-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] unsolicited-report-interval [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] unsolicited-report-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] router-timeout [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] router-timeout
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] source-timeout [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] source-timeout
ip multicast [vlan *vlan_id*[-*vlan_id2*]] querying {enable | disable} [static-source-ip *ip_address*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*]] querying [static-source-ip]
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] robustness [*robustness*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] robustness
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] spoofing {enable | disable}
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] spoofing
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] spoofing static-source-ip *ip_address*
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] spoofing static-source-ip
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*] zapping [{enable | disable}]

no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] zapping
ip multicast [vlan *vlan_id*[-*vlan_id2*] **| service** *service_id*[-*service_id2*]] querier-forwarding [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] **| service** *service_id*[-*service_id2*]] querier-forwarding
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] proxying [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] proxying
ip multicast [vlan *vlan_id*[-*vlan_id2*] helper-address ip_address
no ip multicast [vlan *vlan_id*[-*vlan_id2*] helper-address
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** zero-based-query [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** zero-based-query
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** forward-mode {asm | ssm | mac | auto}
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** forward-mode
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] update-delay-interval *milliseconds*
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] update-delay-interval
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** fast-join [enable | disable]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** fast-join
ip multicast host-list host_list_name ip_address [ip_address]
no ip multicast host-list host_list_name [ip_address]
ip multicast [vlan *vlan_id*] ssm-map {group_address/prefixLen host_list_name | admin-state {enable | disable}}
no ip multicast [vlan *vlan_id*] ssm-map group_address/prefixLen
ip multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer admin-state {enable | disable}
ip multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer max-packet [*num*]
ip multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer max-flow [*num*]
ip multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer timeout [*seconds*]
ip multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer min-delay [*milliseconds*]
ip multicast display-interface-names
no ip multicast display-interface-names
ip multicast inherit-default-vrf-config
no ip multicast inherit-default-vrf-config
ip multicast profile *profile_name*
no ip multicast profile *profile_name* [admin-state | flood-unknown | version | robustness | ...]
ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] apply-profile *profile_name*
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] appy-profile
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] admin-state [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] admin-state
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** flood-unknown [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** flood-unknown
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] version [*version*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] version
ipv6 multicast **{port** *chassis/slot/port* **|** sap port *sap_id*} max-group [*num*] [action {none | drop | replace}]
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** max-group [num] [action {none | drop | replace}]
ipv6 multicast static-neighbor vlan *vlan_id* {port *chassis/slot/port* | *linkagg* agg_id*}*
ipv6 multicast static-neighbor service *service_id* sap {port | *linkagg} {sap_id*}
no ipv6 multicast static-neighbor vlan *vlan_id* {port *chassis/slot/port* | linkagg agg_id}
no ipv6 multicast static-neighbor service *service_id* sap {port | *linkagg} {sap_id*}
ipv6 multicast static-querier vlan *vlan_id* {port *chassis/slot/port* | *linkagg* agg_id*}*
ipv6 multicast static-querier service *service_id* sap {port | *linkagg} {sap_id*}
no ipv6 multicast static-querier vlan *vlan_id* {port *chassis/slot/port* | linkagg agg_id}
no ipv6 multicast static-querier service *service_id* sap {port | *linkagg} {sap_id*}
ipv6 multicast static-group *ipv6_address* vlan *vlan_id* {port *chassis/slot/port* | *linkagg* agg_id*}*
ipv6 multicast static-group *ipv6_address* service *service_id* sap {port | *linkagg} {sap_id*}
no ipv6 multicast static-group *ipv6_address* vlan *vlan_id* {port *chassis/slot/port* | linkagg agg_id}
no ipv6 multicast static-group *ipv6_address* service *service_id* sap {port | *linkagg} {sap_id*}
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*] query-interval [*seconds*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*] query-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** last-member-query-interval [*milliseconds*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]**]** last-member-query-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*] query-response-interval [*milliseconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*] query-response-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] unsolicited-report-interval [*seconds*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] unsolicited-report-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] router-timeout [*seconds*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] router-timeout
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] source-timeout [*seconds*]
no ip multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] source-timeout

ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] querying [{enable | disable}] [static-source-ip *ipv6_address*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] querying [static-source-ip]
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] robustness [*robustness*]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] robustness
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] spoofing {enable | disable}
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*] spoofing
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] spoofing static-source-ip *ipv6_address*
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] spoofing static-source-ip
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] zapping [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] zapping
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] querier-forwarding [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] querier-forwarding
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] proxying [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] proxying
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] helper-address [ipv6_address]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] helper-address
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] zero-based-query [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] zero-based-query
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] forward-mode {asm | ssm | mac | auto}
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] forward-mode
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] update-delay-interval *milliseconds*
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] update-delay-interval
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] fast-join [enable | disable]
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] fast-join
ipv6 multicast host-list host_list_name ipv6_address [ipv6_address]
no ipv6 multicast host-list host_list_name [ipv6_address]
ipv6 multicast [vlan *vlan_id*] ssm-map {group_address[/prefixLen] host_list_name | admin-state {enable | disable}}
no ipv6 multicast ssm-map group_address[/prefixLen]
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer admin-state {enable | disable}
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer max-packet [*num*]
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer max-flow [*num*]
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer timeout [*seconds*]
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*]] initial-packet-buffer min-delay [*milliseconds*]
ipv6 multicast display-interface-names
no ipv6 multicast display-interface-names
ipv6 multicast inherit-default-vrf-config
no ipv6 multicast inherit-default-vrf-config
ipv6 multicast profile *profile_name*
no ipv6 multicast profile *profile_name* [admin-state | flood-unknown | version | robustness | ...]
ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] apply-profile *profile_name*
no ipv6 multicast [vlan *vlan_id*[-*vlan_id2*] | service *service_id*[-*service_id2*]] appy-profile
show ip multicast [vlan *vlan_id* | service *service_id*]
show ip multicast {port [chassis/slot/port] | sap port [*sap_id*]}
show ip multicast forward [*ip_address*] [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ip multicast neighbor [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ip multicast querier [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ip multicast group [*ip_address*] [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ip multicast source [*ip_address*] [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*] [all-vrf]
show ip multicast tunnel [*ip_address*] [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ip multicast host-list [*host_list_name*]
show ip multicast ssm-map [vlan *vlan_id*]
show ip multicast bridge [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*] | *ip_address* | *mac_address*] [all-vrf]
show ip multicast bridge-forward [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*] | *ip_address* | *mac_address*] [all-vrf]
show ip multicast bidir-forward [*ip_address*] [all-vrf]
show ip multicast profile [*profile_name*]
show ipv6 multicast {port [chassis/slot/port] | sap port [*sap_id*]}
show ipv6 multicast forward [*ipv6_ddress*] [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ipv6 multicast neighbor [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ipv6 multicast querier [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]]

show ipv6 multicast group [*ipv6_ddress*] [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ipv6 multicast source [*ipv6_ddress*] [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ipv6 multicast tunnel [*ipv6_address*] [vlan [*vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*]] [all-vrf]
show ipv6 multicast host-list [*host_list_name*]
show ipv6 multicast ssm-map [vlan *vlan_id*]
show ipv6 multicast bridge [vlan *vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*] | *ipv6_address* | *mac_address*] [all-vrf]
show ipv6 multicast bridge-forward [vlan *vlan_id*[-*vlan_id2*] | service [*service_id*[-*service_id2*] | *ipv6_address* | *mac_address*] [all-vrf]
show ipv6 multicast bidir-forward [*ipv6_address*] [all-vrf]
show ipv6 multicast profile [*profile_name*]

DVMRP Commands

ip load dvmrp
ip dvmrp admin-state {enable | disable}
ip dvmrp flash-interval *seconds*
ip dvmrp graft-timeout *seconds*
ip dvmrp interface {*interface_name*}
no ip dvmrp interface {*interface_name*}
ip dvmrp interface *interface_name* metric *value*
ip dvmrp interface *interface_name* mbr-default-information {enable | disable}
ip dvmrp neighbor-interval *seconds*
ip dvmrp neighbor-timeout *seconds*
ip dvmrp prune-lifetime *seconds*
ip dvmrp prune-timeout *seconds*
ip dvmrp report-interval *seconds*
ip dvmrp route-holddown *seconds*
ip dvmrp route-timeout *seconds*
ip dvmrp subord-default {true | false}
show ip dvmrp
show ip dvmrp interface [*ip_address* | *interface_name* | enabled | disabled]
show ip dvmrp neighbor [*ip_address*]
show ip dvmrp nexthop [*ip_address ip_mask*]
show ip dvmrp prune [*group_address source_address source_mask*]
show ip dvmrp route [*ip_address ip_mask*]
show ip dvmrp tunnel [*local_address remote_address*]

PIM Commands

ip load pim
ip pim sparse admin-state {enable | disable}
ip pim bidir admin-state {enable | disable}
ip pim dense admin-state {enable | disable}
ip pim rp-hash admin-state {enable | disable}
ip pim ssm group *group_address/prefix_length* [[no] override] [priority *priority*]
no ip pim ssm group *group_address/prefix_length*
ip pim dense group *group_address/prefix_length* [[no] override] [priority *priority*]
no ip pim dense group *group_address/prefix_length*
ip pim cbsr *ip_address* [priority *priority*] [mask-length *bits*]
no ip pim cbsr *ip_address*
ip pim static-rp *group_address/prefix_length rp_address* [[no] bidir] [[no] override] [priority *priority*]
no ip pim static-rp *group_address/prefix_length rp_address*
ip pim anycast-rp *anycast_rp_address rp_address*
no ip pim anycast-rp *anycast_rp_address rp_address*
ip pim candidate-rp *rp_address group-address/prefix_length* [[no] bidir] [priority *priority*] [interval *seconds*]
no ip pim candidate-rp *rp_address group-address/prefix_length*
ip pim rp-threshold *bps*
ip pim keepalive-period *seconds*
ip pim max-rps *number*
ip pim probe-time *seconds*
ip pim register checksum {header | full}
ip pim register-suppress-timeout *seconds*
ip pim register-rate-limit *pps*
ip pim spt admin-state {enable | disable}
ip pim state-refresh-interval *seconds*
ip pim state-refresh- limit *ticks*
ip pim state-refresh- ttl *num*
ip pim interface *if_name*
ip pim neighbor-loss-notification-period *seconds*
ip pim invalid-register-notification-period *seconds*
ip pim invalid-joinprune-notification-period *seconds*
ip pim rp-mapping-notification-period *seconds*
ip pim interface-election-notification-period *seconds*
ip pim nonbidir-hello-notification-period *seconds*
ip pim df-abort {enable | disable}
ip pim mbr all-sources
no ip pim mbr all-sources
ip pim df-periodic-interval *seconds*
ip pim bfd-state {enable | disable}

ip pim bfd-state all-interfaces {enable | disable}
ip pim interface if_name bfd-state {enable | disable}
ip pim bidir ssm-compat {enable | disable}
ip pim bidir fast-join {enable | disable}
ip pim sparse asm-fast-join {enable | disable}
ip pim sparse ssm-fast-join {enable | disable}
ip pim joinprune-packing {enable | disable}
show ip pim sparse
show ip pim dense
show ip pim ssm group
show ip pim dense group
show ip pim neighbor [*ip_address*]
show ip pim candidate-rp
show ip pim group-map [bsr | static-rp | ssm | dense]
show ip pim interface [*if_name*]
show ip pim static-rp
show ip pim anycast-rp
show ip pim cbsr
show ip pim bsr
show ip pim notifications
show ip pim groute [group_address]
show ip pim sgroute [source_address group_address]
show ip pim df-election [rp_address | if_name]
ipv6 pim sparse admin-state {enable | disable}
ipv6 pim bidir admin-state {enable | disable}
ipv6 pim dense admin-state {enable | disable}
ipv6 pim ssm group *group_address/prefix_length* [[no] override] [priority *priority*]
no ipv6 pim ssm group *group_address/prefix_length*
ipv6 pim dense group *group_address/prefix_length* [[no] override] [priority *priority*]
no ipv6 pim dense group *group_address/prefix_length*
ipv6 pim cbsr *ipv6_address* [priority *priority*] [mask-length *bits*]
no ipv6 pim cbsr *ipv6_address*
ipv6 pim static-rp *group_address/prefix_length rp_address* [[no] bidir] [[no] override] [priority *priority*]
no ipv6 pim static-rp *group_address/prefix_length rp_address*
ipv6 pim anycast-rp *anycast_rp_address rp_address*
no ipv6 pim anycast-rp *anycast_rp_address rp_address*
ipv6 pim candidate-rp *rp_address group_address/prefix_length* [[no] bidir] [priority *priority*] [interval *seconds*]
no ipv6 pim candidate-rp *rp_address group_address/prefix_length*
ipv6 pim rp-switchover {enable | disable}
ipv6 pim register-rate-limit *pps*
ipv6 pim spt admin-state {enable | disable}
ipv6 pim interface *if_name*
ipv6 pim bfd-state {enable | disable}
ipv6 pim bfd-state all-interfaces {enable | disable}
ipv6 pim interface if_name bfd-state {enable | disable}
ipv6 pim bidir ssm-compat {enable | disable}
ipv6 pim bidir fast-join {enable | disable}
ipv6 pim sparse asm-fast-join {enable | disable}
ipv6 pim sparse ssm-fast-join {enable | disable}
ipv6 pim joinprune-packing {enable | disable}
show ipv6 pim sparse
show ipv6 pim dense
show ipv6 pim ssm group
show ipv6 pim dense group
show ipv6 pim interface [*if_name*]
show ipv6 pim neighbor [*ipv6_address*] [*if_name*]
show ipv6 pim static-rp
show ipv6 pim anycast-rp
show ipv6 pim group-map [bsr | static-rp | ssm | dense]
show ipv6 pim candidate-rp
show ipv6 pim cbsr
show ipv6 pim bsr
show ipv6 pim groute [group_address]
show ipv6 pim sgroute [source_address group_address]
show ipv6 pim df-election [rp_address | if_name]

Multicast Routing Commands

ip mroute-boundary *if_name scoped_address mask*
no ip mroute-boundary *if_name scoped_address mask*
ip mroute-boundary extended {enable | disable}
ip mroute interface *if_ name* ttl *threshold*
ip mroute mbr admin-state {enable | disable}
ipv6 mroute interface *if_name* ttl *threshold*
show ip mroute-boundary
show ip mroute
show ipv6 mroute
show ip mroute interface [*interface_name*]
show ipv6 mroute interface {*interface_name*}
show ip mroute-nexthop
show ipv6 mroute-nexthop
show ip mroute mbr

QoS Commands

qos {enable | disable}
qos trust-ports
qos no trust-ports
qos forward log
qos no forward log
qos log console
qos no log console
qos log lines *lines*
qos log level *level*
qos no log level
qos stats interval *seconds*
qos phones [priority *priority_value* | trusted]
qos no phones
qos quarantine mac-group *mac_group*
qos no quarantine mac-group
qos user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}
qos no user-port {filter | shutdown}
qos dei {ingress | egress}
qos no dei {ingress | egress}
debug qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress]
debug no qos
debug no qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress]
debug qos internal [slice *slot/slice*] [flow] [queue] [port] [l2tree] [l3tree] [vector] [pending] [verbose] [mapper] [pool] [log] [pingonly | nopingonly]
clear qos log
qos apply
qos revert
qos flush
qos reset
qos stats reset
qos switch-group {expanded | compact}
qos port *chassis/slot/port*[*-port2*] reset
qos port *chassis/slot/port*[*-port2*]
qos port *chassis/slot/port*[*-port2*] trusted
qos port *chassis/slot/port* no trusted
qos port *chassis/slot/port*[*-port2*] maximum egress-bandwidth *bps*[k | m | g | t]
qos port *chassis/slot/port*[*-port2*] no maximum egress-bandwidth
qos port *chassis/slot/port*[*-port2*] maximum ingress-bandwidth *bps*[k | m | g | t]
qos port *chassis/slot/port*[*-port2*] no maximum ingress-bandwidth
qos port *chassis/slot/port*[*-port2*] maximum {ingress | egress}-depth *bytes* [k | m | g | t]
qos port *chassis/slot/port*[*-port2*] no maximum {ingress | egress}-depth
qos port *chassis/slot/port*[*-port2*] default 802.1p *value*
qos port *chassis/slot/port*[*-port2*] default dscp *value*
qos port *chassis/slot/port*[*-port2*] default classification {tos | 802.1p | dscp}
qos port *chassis/slot/port* dei {ingress | egress}
qos port *chassis/slot/port* no dei {ingress | egress}
qos qsp {qsp_id | qsp_name} import qsp {import_qsp_id | import_qsp_name}
no qos qsp {qsp_id | qsp_name}
qos qsp {qsp_id | qsp_name} qp *qp_id* {pir % | weight weight | scheduler {sp | wrr | wrr2}}
qos qsi {port *chassis/slot/port*[*-port2*] | linkagg *agg_id*[*-agg_id2*] | vf-link *vfl_id*} qsp {*qsp_id* | *qsp_name*}
qos qsp system-default {*qsp_id* | *qsp_name*}
qos qsi {port *chassis/slot/port*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} stats {admin-state {enable | disable} | interval *interval_time*}]}
show qos port [*chassis/slot/port*]
show qos slice [*slot*/*slice*]
show qos log
show qos config
show qos statistics
show qos qsi [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] summary
show qos qsp [*qsp_id* | *qsp_name*] [brief | detail [port *chassis/slot/port*[*-port2*]] | linkagg *agg_id*[*-agg_id2*]]]
show qos wrp [*wrp_id* | *wrp_name*] [detail [port *chassis/slot/port*[*-port2*]] | slot *slot* | linkagg *agg_id*[*-agg_id2*]]]
show qos qsi [port *chassis/slot/port*[*-port2*] | linkagg *agg_id*[*-agg_id2*] | vf-link *vfl_id*] [detail | summary]
show qos qsi {port chassis/slot/port[-port2] | linkagg *agg_id*[*-agg_id2*]} stats [bytes | rate [bytes]]
show qos qsi {port *chassis/slot/port*[*-port2*] | slot *slot* | linkagg *agg_id*[*-agg_id2*]} wred-stats [rate | bytes]
show qos qsp system-default
clear qos qsi {port *chassis/slot/port*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} stats
qos qsp dcb {dcp_id | dcp_name} import qsp dcb {import_dcp_id | import_dcp_name} [802.3x-pause]
no qos qsp dcb {dcp_id | dcp_name}
qos qsp dcb {dcp_id | dcp_name} tc tc_num {pfc flow-type { ll | nll} | pfc link-delay allowance | min-bw % | max-bw % | recommended bw %}
qos qsp dcb {dcp_id | dcp_name} tc-numbering tc_num
qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} qsp dcb {*dcp_id* | *dcb_name*}
qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb dcbx version {ieee | cee | auto}

qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb dcbx admin-state {enable | disable}
qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb dcbx ets [config-tlv {enable | disable} | recommend-tlv {enable | disable} | willing {yes | no}]
qos qsi {port chassis/slot/port[-*port2*] | linkagg agg_id[-agg_id2]} dcb dcbx pfc [config-tlv {enable | disable} | defense {enable | disable} | willing {yes | no}]
show qos qsp dcb [dcp_id | dcp_name] [tc tc_num]
show qos qsi [port chassis/slot/port**[**-*port2***]** | linkagg *agg_id[-agg_id2*]] dcb dcbx [status]
show qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb ets [tc [*tc_num*]]
show qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb pfc
show qos pfc-lossless-usage
show qos qsi [port chassis/slot/port[-port2] dcb pfc stats
clear qos qsi {port *chassis/slot/port*[-*port2*]} dcb pfc stats

QoS Policy Commands

policy rule *rule_name* [enable | disable] [precedence *precedence*] [condition *condition*] [action *action*] [validity-period *name*] [save] [log [log-interval *seconds*]] [count {packets | bytes}] [trap] [default-list]
policy rule *rule_name* no {validity-period | save | log | trap | default-list}
no policy rule *rule_name*
policy validity-period *name* [days *days*] [months *months*] [hours *hh:mm* to *hh:mm*] [interval *mm:dd:yy hh:mm* to *mm:dd:yy hh:mm*]
policy validity-period *name* no {hours | interval}
no policy validity-period *name*
policy list *list_name* type {unp | egress | appfp | empacl} [enable | disable]
no policy list *list_name*
policy list *list_name* rules *rule_name* [*rule_name2*...]
policy list *list_name* **no rules** *rule_name* [*rule_name2*...]
policy network group *net_group ip_address* [mask *net_mask*] [*ip_address2* [mask *net_mask2*]...]
no policy network group *net_group*
policy network group *net_group* no *ip_address* [mask *netmask*] [*ip_address2* [mask *net_mask2*]...]
policy service group *service_group service_name1* [*service_name2*...]
no policy service group *service_group*
policy service group *service_group* no *service_name1* [*service_name2*...]
policy mac group *mac_group mac_address* [mask *mac_mask*] [*mac_address2* [mask *mac_mask2*]...]
no policy mac group *mac_group*
policy mac group *mac_group* no *mac_address* [mask *mac_mask*] [*mac_address2* [mask *mac_mask2*]...]
policy port group *group_name* {*chassis//slot/port*[-*port2*] | *agg_id[-agg_id2*]} [*chassis//slot/port*[-*port2*] | *agg_id[-agg_id2*]]
no policy port group *group_name*
policy port group *group_name* no {*chassis//slot/port*[-*port2*] | *agg_id[-agg_id2*]} [*chassis//slot/port*[-*port2*] | *agg_id[-agg_id2*]]
policy map group *map_group* {*value1*:*value2*...}
no policy map group *map_group*
policy map group no {*value1*:*value2*...}
policy service *service_name*
no policy service *service_name*
policy service *service_name* protocol *protocol* {[source ip-port *port*[-*port*]] [destination ip-port *port*[-*port*]]}
no policy service *service_name*
policy service *service_name* no {source ip-port | destination ip-port}
policy service *service_name* source tcp-port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no source tcp-port
policy service *service_name* destination tcp-port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no destination tcp-port
policy service *service_name* source udp-port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no source udp-port
policy service *service_name* destination udp-port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no destination udp-port
policy condition *condition_name*
no policy condition *condition_name*
policy condition *condition_name* source ip *ip_address* [mask *netmask*]
policy condition *condition_name* no source ip
policy condition *condition_name* source ipv6 {any | *ipv6_address* [mask *netmask*]}
policy condition *condition_name* no source ipv6
policy condition *condition_name* destination ip *ip_address* [mask *netmask*]
policy condition *condition_name* no destination ip
policy condition *condition_name* destination ipv6 {any | *ipv6_address* [mask *netmask*]}
policy condition *condition_name* no destination ipv6
policy condition *condition_name* multicast ip *ip_address* [mask *netmask*]
policy condition *condition_name* no multicast ip
policy condition *condition_name* source network group *network_group*
policy condition *condition_name* no source network group
policy condition *condition_name* destination network group *network_group*
policy condition *condition_name* no destination network group
policy condition *condition_name* multicast network group *multicast_group*
policy condition *condition_name* no multicast network group
policy condition *condition_name* source ip-port *port*[-*port*]
policy condition *condition_name* no source ip-port

policy condition *condition_name* destination ip-port *port*[*-port*]
policy condition *condition_name* no destination ip-port
policy condition *condition_name* source tcp-port *port*[*-port*]
policy condition *condition_name* no source tcp-port
policy condition *condition_name* destination tcp-port *port*[*-port*]
policy condition *condition_name* no destination tcp-port
policy condition *condition_name* source udp-port *port*[*-port*]
policy condition *condition_name* no source udp-port
policy condition *condition_name* destination udp-port *port*[*-port*]
policy condition *condition_name* no destination udp-port
policy condition *condition_name* ethertype *etype*
policy condition *condition_name* no ethertype
policy condition *condition_name* established
policy condition *condition_name* no established
policy condition *condition_name* tcpflags [any | all] {f | s | r | p | a | u | e | w} mask {f | s | r | p | a | u | e | w}
policy condition *condition_name* no tcpflags
policy condition *condition_name* service *service_name*
policy condition *condition_name* no service
policy condition *condition_name* service group *service_group*
policy condition *condition_name* no service group
policy condition *condition_name* icmptype *type*
policy condition *condition_name* no icmptype
policy condition *condition_name* icmpcode *code*
policy condition *condition_name* no icmpcode
policy condition *condition_name* ip-protocol *protocol*
policy condition *condition_name* no ip-protocol
policy condition *condition_name* ipv6
policy condition *condition_name* no ipv6
policy condition *condition_name* flow-label *flow_label_value*
policy condition *condition_name* no flow-label
policy condition *condition_name* tos *tos_value* [mask *tos_mask*]
policy condition *condition_name* no tos
policy condition *condition_name* dscp {*dscp_value*[*-value*]} [mask *dscp_mask*]
policy condition *condition_name* no dscp
policy condition *condition_name* source mac *mac_address* [mask *mac_mask*]
policy condition *condition_name* no source mac
policy condition *condition_name* destination mac *mac_address* [mask *mac_mask*]
policy condition *condition_name* no destination mac
policy condition *condition_name* source mac group *group_name*
policy condition *condition_name* no source mac group
policy condition *condition_name* destination mac group *mac_group*
policy condition *condition_name* no destination
policy condition *condition_name* source vlan *vlan_id*
policy condition *condition_name* no source vlan
policy condition *condition_name* inner source-vlan *vlan_id*
policy condition *condition_name* no inner source-vlan
policy condition *condition_name* destination vlan *vlan_id*
policy condition *condition_name* no destination vlan
policy condition *condition_name* 802.1p *802.1p_value*
policy condition *condition_name* no 802.1p
policy condition *condition_name* inner 802.1p *802.1p_value*
policy condition *condition_name* no inner 802.1p
policy condition *condition_name* source {port *chassis/slot/port*[*-port2*] | linkagg *agg_id[-agg_id2*]}
policy condition *condition_name* no source {port | linkagg}
policy condition *condition_name* destination {port *chassis/slot/port*[*-port2*] | linkagg *agg_id[-agg_id2*]}
policy condition *condition_name* no destination {port | linkagg}
policy condition *condition_name* source port group *group_name*
policy condition *condition_name* no source port group
policy condition *condition_name* destination port group *group_name*
policy condition *condition_name* no destination port
policy condition *condition_name* vrf {*vrf_name* | default}
policy condition *condition_name* no vrf
policy condition *condition_name* fragments
policy condition *condition_name* no fragments
policy condition *condition_name* appfp-group *group_name*
policy condition *condition_name* no appfp-group
policy condition *condition_name* vxlan vni *vxlan_id*
no policy condition *condition_name*
policy condition *condition_name* vxlan inner source mac *mac_address* [mask *mac_mask*]
policy condition *condition_name* vxlan no source mac
policy condition *condition_name* vxlan inner source mac-group *group_name*
policy condition *condition_name* vxlan no source mac-group
policy condition *condition_name* vxlan inner source ip *ip_address* [mask *netmask*]
policy condition *condition_name* vxlan no source ip
policy condition *condition_name* vxlan inner source ipv6 *ipv6_address* [mask *netmask*]
policy condition *condition_name* vxlan no source ipv6
policy condition *condition_name* vxlan inner ip-protocol *protocol*
policy condition *condition_name* vxlan no ip-protocol
policy condition *condition_name* vxlan inner l4-port {src *src_port* | dest *dest_port*}
policy condition *condition_name* vxlan no l4-port
policy condition *condition_name* vxlan vxlan-port *udp_port*
policy condition *condition_name* vxlan no vxlan-port
policy action *action_name*
policy no action *action_name*
policy action *action_name* disposition {accept | drop | deny}

policy action *action_name* no disposition
policy action *action_name* shared
policy action *action_name* no shared
policy action *action_name* priority *priority_value*
policy action *action_name* no priority
policy action *action_name* maximum bandwidth *bps*[k | m | g | t]
policy action *action_name* no maximum bandwidth
policy action *action_name* maximum depth *bytes* [K (kilo)| M (mega) | G (giga) | T (tera)]
policy action *action_name* no maximum depth
policy action action_name cir bps [cbs bytes] [pir bps] [pbs bytes] [color-only]
policy action action_name no cir
policy action action_name no pir
policy action action_name cpu priority *priority*
policy action action_name no cpu priority
policy action *action_name* tos *tos_value*
policy action *action_name* no tos
policy action *action_name* 802.1p *802.1p_value*
policy action *action_name* no 802.1p
policy action *action_name* dscp *dscp_value*
policy action *action_name* no dscp
policy action map {802.1p | tos | dscp} to {802.1p | tos | dscp} using *map_group*
policy action no map
policy action *action_name* permanent gateway-ip *ip_address*
policy action *action_name* no permanent gateway-ip
policy action *action_name* permanent gateway-ipv6 *ipv6_address*
policy action *action_name* no permanent gateway-ipv6
policy action *action_name* port-disable
policy action *action_name* no port-disable
policy action *action_name* redirect port *chassis/slot/port*
policy action *action_name* no redirect port
policy action *action_name* redirect linkagg *agg_id*
policy action *action_name* no redirect linkagg
policy action *action_name* no-cache
policy action *action_name* no no-cache
policy action *action_name* [ingress | egress | ingress egress] mirror {*chassis/slot/port* | session *session_id}*
policy action *action_name* no mirror *{chassis/slot/port* | session *session_id}*
show [applied] policy network group [*network_group*]
show [applied] policy service [*service_name*]
show [applied] policy service group [*service_group*]
show [applied] policy mac group [*mac_group*]
show [applied] policy port group [*group_name*]
show [applied] policy map group [*group_name*]
show [applied] policy action [*action_name*]
show [applied] policy condition [*condition_name*]
show active policy rule [*rule_name*]
show [applied] policy rule [*rule_name*]
show policy validity period [*name*]
show active policy list [*list_name*]
show [applied] policy list [*list_name*]
show policy ipv4-summary [rule *rule_name*]
show policy ipv6-summary [rule *rule_name*]

Policy Server Commands

policy server load
policy server flush
policy server *ip_address* [port *port_number*] [admin-state {enable | disable}] [preference *preference*] [user *user_name* password *password*] [searchbase *search_string*] [ssl | no ssl]
no policy server *ip_address* [port *port_number*]
show policy server
show policy server long
show policy server statistics
show policy server rules
show policy server events

AAA Commands

aaa radius-server *server_name* host {*hostname* | *ip_address* | *ipv6_address*} [*hostname2* | *ip_address2* | *ipv6_address2*] {key *secret* | hash-key hash_*secret* | prompt-key}[salt *salt* | hash-salt *hash_salt*] [retransmit *retries*] [timeout *seconds*] [auth-port *auth_port*] [acct-port *acct_port*] [vrf-name name] [ssl | no ssl]
no aaa radius-server *server_name*
aaa radius-server *server_name* health-check [poling-interval *seconds* | username user_name | password password | hash-key *hash_secret* | failover]
no aaa radius-server *server_name* health-check [failover]
aaa radius unp-profile-precedence {tunnel-private-group-id | filter-id}
aaa test-radius-server *server_name* type {authentication user user_name password password [method {md5 | pap}] | accounting user user_name}
aaa tacacs+-server *server_name* host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*] {key *secret* | prompt-key}[salt *salt* | hash-salt *hash_salt*] [timeout *seconds*] [port *port*] [vrf-name name]
no aaa tacacs+-server *server*
aaa tacacs command-authorization {enable | disable}

aaa ldap-server *server_name* host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*] dn *dn_name* {password *super_password* | *prompt-password}*[salt *salt* | hash-salt *hash_salt*] [base *search_base*] [retransmit *retries*] [timeout *seconds*] [ssl | no ssl] [port *port*] [vrf-name name]
no aaa ldap-server *server-name*
system fips admin-state {enable | disable}
aaa authentication {console | telnet | ftp | http | snmp | ssh | default} *server1* [*server2*...] [local]
no aaa authentication [console | telnet | ftp | http | snmp | ssh | default]
aaa console admin-only {enable | disable}
aaa authentication {console | telnet | ftp | http | snmp | ssh} default
aaa accounting session *server1* [*server2*...] [local]
no accounting session
aaa accounting command *server1* [*server2*...] [local]
no accounting command
aaa device-authentication {802.1x | mac | captive-portal} *server1* [*server2*] [*server3*] [*server4*]
no device-authentication {802.1x | mac | captive-portal}
aaa accounting {802.1x | mac | captive-portal} {*server1* [*server2*...] | syslog *ip_address* [port *udp_port*]}
no accounting {802.1x | mac | captive-portal}
aaa accounting {802.1x | mac | captive-portal} radius calling-station-id {mac-address | ip-address}
aaa 802.1x re-authentication {enable | disable | interval *seconds* | trust-radius {enable | disable}}
aaa {802.1x | mac | captive-portal} interim-interval *seconds* [trust-radius {enable | disable}]
aaa {mac | captive-portal} session-timeout {enable | disable} [interval *seconds*] [trust-radius {enable | disable}]
aaa session console {enable | disable}
aaa {mac | captive-portal} inactivity-logout {enable | disable} [interval *seconds*]
aaa radius nas-port-id {user-string *string* | default}
aaa radius nas-identifier {user-string *string* | default}
aaa radius nas-ip-address {default | local-ip [*ip_address*]}
aaa radius mac-format {username | password | calling-station-id | called-station-id} delimiter {*char* | none} case {uppercase | lowercase}
aaa profile *profile_name*
no aaa profile *profile_name*
user *username*
no user *username*
password
user password-size min *size*
user password-expiration {*day* | disable}
user password-policy cannot-contain-username {enable | disable}
user password-policy min-uppercase *number*
user password-policy min-uppercase *number*
user password-policy min-digit *number*
user password-policy min-nonalpha *number*
user password-history *number*
user password-min-age *days*
user lockout-window *minutes*
user lockout-threshold *number*
user lockout-duration *minutes*
user *username* {lockout | unlock}
show aaa server [*server_name*]
show aaa server *server_name* statistics
aaa radius-server *server_name* clear-statistics
show aaa authentication
show aaa device-authentication [802.1x | mac | captive-portal]
show aaa accounting [802.1x | mac | captive-portal]
show aaa {802.1x | mac | captive-portal} config
show aaa radius config
show aaa radius health-chec-config
show aaa profile [*profie_name*]
show aaa session console config
show user [*username*]
show user password-policy
show user lockout-setting
show aaa priv hexa [*domain or family*]
show system fips
aaa switch-access mode {default | enhanced}
aaa switch-access ip-lockout-threshold number
aaa switch-access banned-ip {all | ip_address} release
aaa switch-access priv-mask {console | telnet | ssh | http | https} {read-only | read-write} [*families...* | *domains...*| all | none | all-except *families...*]
aaa switch-access management-stations admin-state {enable | disable}
aaa switch-access management-stations [ip_address | ip_address /mask]
no aaa switch-access management-stations ip_address
show aaa switch-access mode
show aaa switch-access ip-lockout-threshold
show aaa switch-access banned-ip
show aaa switch-access priv-mask
show aaa switch-access management-stations
show aaa switch-access hardware-self-test
show aaa switch-access process-self-test
aaa common-criteria admin-state {enable | disable}
show aaa common-criteria config
aaa certificate update-ca-certificate ca_file
aaa certificate update-crl crl_file
aaa certificate generate-rsa-key key-file key_file

aaa certificate generate-self-signed {cert_file} key {key_file} [days valid_period} {CN common_name} {ON org_name} {OU org_unit} {L locality} {ST state} {C country}
aaa certificate view cert_file
aaa certificate verify ca-certificate cert_file certificate cert_file
aaa certificate delete cert_file
aaa certificate generate-csr {csr_file} key {key_file} [dn domain_name} {CN common_name} {ON org_name} {OU org_unit} {L locality} {ST state} {C country}
ssl pki client validate-certificate admin-state {enable | disable}
ssl pki client mutual-authentication admin-state {enable | disable}
ssl pki server mutual-authentication admin-state {enable | disable}
ssl pki tls version {1.0 | 1.1 | 1.2}
show ssl pki config
ssl cipher {[level {all | high | medium | low}] | [custom {*string* | *file string*}]}
show ssl ciphers all
show ssl ciphers config
kerberos inactivity-timer num
kerberos ip-address ip_address [port num]
no kerberos ip-address ip_address
kerberos server-timeout num
kerberos authentication-pass policy-list-name policy_list
no kerberos authentication-pass policy-list-name
kerberos authentication-pass domain domain_name policy-list-name policy_list
no kerberos authentication-pass domain domain_name
clear kerberos statistics
show kerberos configuration
show kerberos users [port chassis/slot/port |linkagg *agg_id* | mac-address *mac_address* | count]
show kerberos statistics
aaa jitc admin-state {enable | disable}
show aaa jitc config

Access Guardian Commands

unp dynamic-vlan-configuration
no unp dynamic-vlan-configuration
unp dynamic-profile-configuration
no unp dynamic-profile-configuration
unp delay-learning *seconds*
unp auth-server-down {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp auth-server-down [profile1] [profile2] [profile3]
unp auth-server-down-timeout *seconds*
no unp auth-server-down-timeout
unp policy validity-period *policy_name* [days *days*] [months *months*] [hours *hh:mm* to *hh:mm*] [interval *mm:dd:yy hh:mm* to *mm:dd:yy hh:mm*] [timezone *zones*]
no unp policy validity-period *policy_name* [days *days* | months *months* | hours | interval | timezone]
unp policy validity-location *policy_name* [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*] [system-name *system_name*] [system-location *system_location*]
no unp policy validity-location *policy_name* [port | linkagg | system-name | system-location]
unp domain *domain_id* [description *domain_description*]
no unp domain *domain_id* description *domain_description*
unp redirect pause-timer *seconds*
no redirect pause-timer
unp redirect proxy-server-port *proxy_port*
no unp rediret proxy-server-port
unp redirect-server {*ip_address* | *domain_name*}
no unp redirect-server
unp redirect allowed-name *name* ip-address *ip_address* ip-mask *ip_mask*
no unp redirect allowed-name *name*
unp [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] force-l3-learning [port-bounce]
no unp [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] force-l3-learning [port-bounce]
unp 802.1x-pass-through
no unp 802.1x-pass-through
unp ipv6-drop
no unp ipv6-drop
unp ap-mode {enable | disable}
unp mac-mobility
no unp mac-mobility
unp user flush [port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] [sap-id [linkagg] *sap_id*] [service-id *service_id*] [authentication-type {mac | 802.1x | none} [profile *profile_name*] [mac-address *mac_address*]
unp profile *profile_name*
no unp profile *profile_name*
unp profile *profile_name* qos-policy-list *list_name*
no unp profile *profile_name* qos-policy-list
unp profile *profile_name* location-policy *policy_name*
no unp profile *profile_name* location-policy
unp profile *profile_name* period-policy *policy_name*
no unp profile *profile_name* period-policy
unp profile *profile_name* captive-portal-authentication
no unp profile *profile_name* captive-portal-authentication
unp profile *profile_name* captive-portal-profile *cp_profile_name*
no unp profile *profile_name* captive-portal-profile
unp profile *profile_name* kerberos-authentication

no unp profile *profile_name* kerberos-authentication
unp profile *profile_name* authentication-flag
no unp profile *profile_name* authentication-flag
unp profile *profile_name* mobile-tag
no unp profile *profile_name* mobile-tag
unp profile *profile_name* maximum-ingress-bandwidth *bps*[k | m]
no unp profile *profile_name* maximum-ingress-bandwidth
unp profile *profile_name* maximum-egress-bandwidth *bps*[k | m]
no unp profile *profile_name* maximum-egress-bandwidth
unp profile *profile_name* maximum-ingress-depth *bytes*
no unp profile *profile_name* maximum-ingress-depth
unp profile *profile_name* maximum-egress-depth *bytes*
no unp profile *profile_name* maximum-egress-depth
unp profile *profile_name* inactivity-interval *seconds*
unp profile *profile_name* mac-mobility
no unp profile *profile_name* mac-mobility
unp profile *profile_name* saa-profile *profile_name*
no unp profile *profile_name* saa-profile
unp profile *profile_name* map vlan *vlan_id*
unp profile *profile_name* map service-type spb tag-value {0 | qtag | outer_qtag:inner_qtag} isid *instance_id* bvlan *bvlan_id* [multicast-mode {headend | tandem}] [vlan-xlation] [igmp-snooping [profile {default | *ipms_profile*}] [mld-snooping [profile {default | *ipms_profile*}]
no unp profile *profile_name* map service-type spb [vlan-xlation] [igmp-snooping [profile]] [mld-snooping [profile]]
unp profile *profile_name* map service-type vxlan tag-value {0 | qtag | outer_qtag:inner_qtag} vnid *vxlan_id* {far-end-ip-list *ip_list_name* [multicast-group *mc_group_address*] | multicast-group *mc_group_address* [far-end-ip-list *ip_list_name*]} [multicast-mode [tandem | headend | hybrid] [vlan-xlation]
no unp profile *profile_name* map service-type vxlan [far-end-ip-list | multicast-group | vlan-xlation]
unp vxlan far-end-ip-list *ip_list_name ip_address* [*ip_address*]
no unp vxlan far-end-ip-list *ip_list_name* [*ip_address* [*ip_address*]]
unp profile *profile_name* map service-type l2gre tag-value {0 | *qtag* | *outer_qtag:inner_qtag*} vpnid *vpn_id* {far-end-ip-list *ip_list_name* | far-end-ip *ip_address*} [port-isolation-disable] [vlan-xlation]
no unp profile *profile_name* map service-type l2gre [far-end-ip-list | far-end-ip | vlan-xlation]
unp l2gre far-end-ip-list *ip_list_name ip_address*
no unp l2gre far-end-ip-list *ip_list_name* [*ip_address*]
unp profile *profile_name* map service-type static tag-value {0 | qtag | outer_qtag:inner_qtag} service-id *service_id*
unp system-default service-mod {*mod_number* | default}
unp system-default service-base {*base_number* | default}
unp system-default multicastmode {tandem | headend | hybrid}
unp system-default vlan-translation {enable | disable}
unp system-default multicastgroup {*mc_group_address* | default}
unp system-default far-end-ip-list {*ip_list_name* | default}
unp saa-profile *profile_name [jitter-threshold jitter_thresh] [latency-threshold latency_thresh]*
no unp saa-profile *profile_name*
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id1*[-*agg_id2*]} port-type {access | bridge}
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id1*[-*agg_id2*]}
unp {port *chassis*/*slot/port***[**-*port2***]** | linkagg *agg_id[-agg_id2*]} l2-profile *l2profile_name*
no unp {port *chassis/slot/port***[**-*port2***]** | linkagg *agg_id[-agg_id2*]} l2-profile
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} redirect port-bounce
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} redirect port-bounce
unp redirect port-bounce {enable | disable}
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication pass-alternate *profile_name*
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*} 802.1X-authentication pass-alternate
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication tx-period *seconds*
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication tx-period
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication supp-timeout *seconds*
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication supp-timeout
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication max-req *max_req*
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication max-req
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication bypass-8021x
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication bypass-8021x
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication failure-policy {mac}
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} 802.1x-authentication failure-policy
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} mac-authentication
no unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} mac-authentication
unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} mac-authentication pass-alternate *profile_name*

no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} mac-authentication pass-alternate
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} mac-authentication allow-eap {pass | fail | noauth}
no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} mac-authentication allow-eap
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} classification
no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} classification
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} trust-tag
no {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} trust-tag
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} default-profile *profile_name*
no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*} default-profile
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} domain *domain_id*
no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} domain *domain_id*
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} aaa-profile *profile_name*
no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} aaa-profile
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} port-template *template_name*
no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} port-template
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} direction {both | in}
no unp {port *chassis//slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} direction
unp {port {*chassis/slot/port1*[*-port2*] | linkagg *agg_id1*[*-agg_id2*]} admin-state {enable | disable}
unp {port [*chassis_id/*]*slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} dynamic-service {spb | vxlan | none}
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} vlan *vlan_id* [*-vlan_id2]* [tagged]
no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} vlan *vlan_id* [*-vlan_id2]*
unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} profile *profile_name*
no unp {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} profile *profile_name*
unp {port *chassis/slot/port*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} ap-mode
no unp {port *chassis/slot/port*[*-port2*] | linkagg *agg_id*[*-agg_id2*]} ap-mode
unp port-template {*template_name* | bridgeDefaultPortTemplate | accessDefaultPortTemplate}
no unp port-template *template_name* [802.1x-authentication | 802.1x authentication pass-alternate | mac-authentication | mac-authentication pass-alternate | ...]
unp network-group *net_group_name ip_address* [mask *net_mask*] [*ip_address2* [mask *net_mask2*]...]
no unp network-group *net_group_name* [*ip_address* [mask *net_mask*] [*ip_address2* [mask *net_mask2*]...]
unp router-auth user-group *user_group_name* {[src-network-group *net_group*] dst-network-group *net_group_name*}
no unp router-auth user-group *user_group_name*
unp router-auth cp-profile *cp_profile_name*
no unp router-auth cp-profile *cp_profile_name*
unp router-auth user flush {user-group *user_group_name* | user-name *cp_user_name* | [ip-address *ipv4_address* | auth-type {cp | ip} | all}
show unp network-group
show unp router-auth user-group [*user_group_name*]
show unp router-auth configuration
show unp router-auth users [user-name *cp_user_name*] [ip-address *ipv4_address*] [auth-type {cp | ip}] [auth-status {pass | fail}]
unp classification {port *chassis/slot/port1*[*-port2*] | linkagg [*agg_id*[*-agg_id2*]} [vlan-tag *vlan_id* | *outer_vlan_id:inner_vlan_id*] {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification {port *chassis/slot/port1*[*-port2*] | linkagg *agg_id*} [profile1] [profile2] [profile3]
unp classification domain *domain_id* [vlan-tag *vlan_id* | *outer_vlan_id:inner_vlan_id*] {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification domain *domain_id* [profile1] [profile2] [profile3]
unp classification mac-address *mac_address* [domain *domain_id*] [vlan-tag *vlan_id* | *outer_vlan_id:inner_vlan_id*] {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification mac-address *mac_address* [profile1] [profile2] [profile3]
unp classification mac-oui *mac_oui* [vlan-tag *vlan_id* | *outer_vlan_id:inner_vlan_id*] {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification mac-oui *mac_oui* [profile1] [profile2] [profile3]
unp classification mac-range *low_mac_address high_mac_address* [domain *domain_id*] [vlan-tag *vlan_id* | *outer_vlan_id:inner_vlan_id*] {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification mac-range *low_mac_address high_mac_address* [profile1] [profile2] [profile3]
unp classification ip-address *ip_address* mask *subnet_mask* [domain *domain_id*] [vlan-tag *vlan_id* | *outer_vlan_id:inner_vlan_id*] {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification ip-address *ip_address* mask *subnet_mask* [profile1] [profile2] [profile3]
unp classification vlan-tag {*vlan_id* | *outer_vlan_id***:***inner_vlan_id***]**} [domain *domain_id*] {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification vlan-tag *vlan_id* [profile1] [profile2] [profile3]
unp classification lldp med-endpoint {ip-phone | access-point} {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification lldp med-endpoint {ip-phone | access-point} [profile1] [profile2] [profile3]
unp classification authentication-type {none | mac [fail] | 802.1x [fail]} [vlan-tag *vlan_id* | *outer_vlan_id:inner_vlan_id*] {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp classification authentication-type {none | mac [fail] | 802.1x [fail]} [profile1] [profile2] [profile3]

unp classification-rule *rule_name* [precedence *precedence_value*] [profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]]
no unp classification-rule *rule_name* [profile1] [profile2] [profile3]
unp classification-rule *rule_name* {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*}
no unp classification-rule *rule_name* {port | linkagg}
unp classification-rule *rule_name* domain *domain_id*
no unp classification-rule *rule_name* domain
unp classification-rule *rule_name* mac-address *mac_address*
no unp classification-rule *rule_name* mac-address
unp classification-rule *rule_name* mac-oui *mac_oui*
no unp classification-rule *rule_name* mac-oui
unp classification-rule *rule_name* mac-range *low_mac_address high_mac_address*
no unp classification-rule *rule_name* mac-range
unp classification-rule *rule_name* ip-address *ip_address* **mask** *subnet_mask*
no unp classification-rule *rule_name* ip-address
unp classification-rule *rule_name* vlan-tag [*vlan_id* | *outer_vlan_id:inner_vlan_id*]
no unp classification-rule vlan-tag
unp classification-rule *rule_name* lldp med-endpoint {ip-phone | access-point}
no unp classification-rule *rule_name* lldp med-endpoint ip-phone
unp classification-rule *rule_name* authentication-type {none | mac [fail] | 802.1x [fail]}
no unp classification-rule *rule_name* authentication-type
unp classification-rule *rule_name* device-type *device_name*
no unp classification-rule *rule_name* device-type
unp user-role *role_name* [precedence *precedence_value*]
no unp user-role *role_name*
unp user-role *role_name* policy-list *list_name*
no unp user-role *role_name* policy-list
unp user-role *role_name* {profile1 *profile_name* [profile2 *profile_name*] [profile3 *profile_name*]}
no unp user-role *role_name* [profile1] [profile2] [profile3]
unp user-role *role_name* authentication-type {none | mac [fail] | 802.1x [fail]}
no unp user-role *role_name* authentication-type
unp user-role *role_name* cp-status-post-login
no unp user-role *role_name* cp-status-post-login
unp restricted-role {unauthorized | qmr | cp-prelogin} policy-list *list_name*
no unp restricted-role {unauthorized | qmr | cp-prelogin} policy-list
captive-portal mode {internal | internal dhcp [ip-lease-time *seconds*] [ip-renew-time *seconds*] [ip-rebinding-time *seconds*] | external}
no captive-portal mode internal
captive-portal name {*ip_address* | *domain_name*}
no captive-portal name
captive-portal ip-address *ip_address*
captive-portal success-redirect-url *redirect_url*
no captive-portal success-redirect-url
captive-portal proxy-server-port *proxy_port*
no captive-portal proxy-server-port
captive-portal retry-count *retries*
captive-portal authentication-pass {policy-list *list_name* | profile *profile_name* | profile-change {enable | disable}}
no captive-portal authentication-pass {policy-list | profile}
captive-portal authentication-pass realm {prefix | suffix} domain *domain_name* {policy-list *list_name* | profile *profile_name* | profile-change {enable | disable}}
no captive-portal authentication-pass [realm {prefix | suffix} domain *domain_name*]
captive-portal-profile *profile_name*
no captive-portal-profile *profile_name*
show captive-portal configuration
show captive-portal {profile-names | profile-name *profile_name* configuration}
qmr quarantine path *url*
no qmr quarantine path
qmr qos quarantine page {enable | disable}
qmr quarantine allowed-name *name* ip-address *ip_address* [ip-mask *ip_mask*]
no qmr quarantine allowed-name *name*
qmr quarantine custom-proxy-port *proxy_port*
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
zeroconf ssdp admin-state {enable | disable}
zeroconf mode [tunnel [type standard] | gateway | responder]
zeroconf responder-ip ip_address
no zeroconf responder-ip ip_address
zeroconf gateway-vlan-list vlan_id1...vlan_idn
no zeroconf gateway-vlan-list vlan_id1...vlan_idn
zeroconf access-vlan-list vlan_id1...vlan_idn
no zeroconf access-vlan-list vlan_id1...vlan_idn
zeroconf server-policy policy_name [role | vlan | location | username | mac-address]
no zeroconf server-policy policy_name [role | vlan | location | username | mac-address]
zeroconf client-policy *policy_name* [role | vlan | location | username | mac-address]
no zeroconf client-policy *policy_name* [role | vlan | location | username | mac-address]
zeroconf service-rule rule_name server-policy *server_policy_name* client-policy *client_policy_name*
no zeroconf service-rule rule_name
zeroconf service-rule rule_name [mdns-service-id | ssdp-service-id] *service_id1.....[service_idn]*
no zeroconf service-rule rule_name [mdns-service-id | ssdp-service-id] *service_id1.....[service_idn]*
zeroconf [mdns service-list | ssdp service-list] service_id1...service_idn
no zeroconf [mdns service-list | ssdp service-list] service_id1...service_idn

zeroconf {mdns | ssdp} service-id service-id query-request
zeroconf edge-ip-list *ip_address*1...ip_addressn
no zeroconf edge-ip-list ip_address1...ip_addressn
zeroconf {mdns | ssdp} refresh-database
show zeroconf
show zeroconf [mdns | ssdp] services
show zeroconf [mdns | ssdp] services-cache
show zeroconf edge-details
show zeroconf server policies
show zeroconf client policies
show zeroconf service rules
show zeroconf [mdns | ssdp] server policy-instances
show unp profile [*profile_name*]
show unp profile [*profile_name*] map {vlan | service-type {spb | vxlan | static | l2gre}}
show unp vxlan far-end-ip-list [*ip_list_name*]
show unp l2gre far-end-ip-list [*ip_list_name*]
show unp saa-profile [*profile_name*]
show unp global configuration
show unp domain
show unp classification *rule_type*
show unp classification-rule [*rule-name*]
show unp user-role [*role_name*]
show unp restricted-role
show unp {port [*chassis/slot/port1*[-*port2*]] | linkagg [*agg_id*[-*agg_id2*]]} [type {bridge | access}]
show unp {port [*chassis/slot/port1*[-*port2*]] | linkagg [*agg_id*[-*agg_id2*]]} config
show unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-*agg_id2*]} bandwidth
show unp {port *chassis/slot/port1*[-*port2*] | linkagg *agg_id*[-agg_id2]} 802.1x statistics
show unp {port [*chassis/slot/port1*[-*port2*]] | linkagg [*agg_id*[-*agg_id2*]} configured-vlans
show unp {port [*chassis/slot/port1*[-*port2*]] | linkagg [*agg_id*[-*agg_id2*]} profile
show unp port-template [*template_name*] [config | configured-vlans | profile]
show unp user [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] [sap-id *sap_id*] [service-id *service_id*] [profile *profile_name*] [authentication-type {none | mac | 802.1x}] [mac-address *mac_address*] [count]
show unp user status [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*] [sap-id *sap_id*] [service-id *service_id*] [profile *profile_name*] [authentication-type {none | mac | 802.1x}] [mac-address *mac_address*]
show unp user details [port *chassis/slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]] [sap-id *sap_id*] [service-id *service_id*] [profile *profile_name*] [authentication-type {none | mac | 802.1x}] [mac-address *mac_address*]
show unp policy validity-period [*policy_name*]
show unp policy validity-location [*policy_name*]
device-profile admin-state {enable | disable}
device-profile [port *chassis/]*slot/port1[-*port2*] | linkagg *agg_id1*[-*agg_id2*] admin-state {enable | disable}
device-profile device-type *type_name* device-name *device_name* from {mac-address *mac_address* | dhcp-option-55 *dhcp_option*}
no device-profile device-type *type_name*
device-profile update-signature
device-profile update-signature from *file-name*
device-profile auto-unp-assignment
no device-profile auto-unp-assignment
show device-profile config
show device-profile summary
show device-profile catalog [unknown]
show device-profile signatures from *file-name*
show device-profile signatures

Application Monitoring and Enforcement Commands

app-mon admin-state {enable | disable}
app-mon {port *chassis*/slot/port[-*port2*] | slot chassis/slot [-slot]} admin-state {enable | disable}
app-mon auto-group create
app-mon app-group app_group_name {add | remove} {app-name app_name | from app_name to app_name}
no app-mon app-group app_group_name
app-mon app-list {enforcement | monitor} {add | remove} {app-name app_name | app-group app_group_name}
app-mon apply
app-mon l3-mode {ipv4 | ipv6} admin-state {enable | disable}
app-mon {port *chassis*/slot/port[-*port2*] | slot chassis/slot} l4-mode {tcp | udp} admin-state {enable | disable}
app-mon l4port-exclude range-id *number* {tcp-service-port | udp-port} start number end number
no app-mon l4port-exclude range-id
app-mon flow-table {enforcement | monitor} flush
app-mon flow-table enforcement stats admin-state {enable | disable}
app-mon aging enforcement app-name app_name [tcp | udp] interval {120m | 60m | 30m | 10m | 5m | 3m | default}
app-mon logging-threshold {enforcement | monitor} num-of-flows {number | default}
app-mon flow-sync enforcement interval {number | default}
app-mon force-flow-sync {enforcement | monitor}
show app-mon config
show app-mon [port *chassis*/slot/port | slot chassis/slot]
show app-mon app-pool
show app-mon app-list {monitor | enforcement} [active [stats]] [conflict]

show app-mon app-group [group-name group_name]
show app-mon app-record [hourly | twenty-four-hours | current-hour] [verbose]
show app-mon ipv4-flow-table {monitor | enforcement [verbose]} [{src-ipv4 | dest-ipv4} *ip_address*] [app-name app_name | app-group grp_name]
show app-mon ipv6-flow-table {monitor | enforcement [verbose]} [{src-ipv6 | dest-ipv6} ip_address] [app-name app_name | app-group grp_name]
show app-mon l4port-exclude range-id [number]
show app-mon stats
show app-mon aging enforcement [app-name app_name]
show app-mon vc-topology
clear app-mon app-list {monitor| enforcement}

Application Fingerprinting Commands

app-fingerprint admin-state {enable | disable}
app-fingerprint {port *chassis/slot/port*[*-port*] | linkagg *agg_id[-agg_id2*]} {monitor-app-group *group_name* | policy-list-name *policy_list* | unp-profile}
no app-fingerprint {port *chassis/slot/port*[*-port*] | linkagg *agg_id[-agg_id2*]}
app-fingerprint signature-file *filename*
app-fingerprint reload-signature-file
app-fingerprint trap {enable | disable|
show app-fingerprint configuration
show app-fingerprint [port *chassis/slot/port* | linkagg *agg_id*]
show app-fingerprint app-name *[app_name*]
show app-fingerprint app-group *[group_name*]
show app-fingerprint database *[*port *chassis/slot/port* | linkagg *agg_id*] [detail]
show app-fingerprint statistics *[*port *chassis/slot/port* | linkagg *agg_id*]

FIP Snooping Commands

fcoe fip-snooping admin-state {enable | disable}
fcoe address-mode {spma | fpma}
fcoe priority {*priority*} [*priority*]
fcoe priority-protection {enable | disable}
fcoe priority-protection action {drop | remark *priority*}
fcoe filtering-resource trap-threshold *percentage*
fcoe house-keeping-time-period *seconds*
fcoe vlan *vlan_id* [admin-state {enable | disable}] [name *description***]**
no fcoe vlan *vlan_id*
fcoe fcf mac *mac_address* vlan *vlan_id*
no fcoe fcf *mac_address* vlan *vlan_id*
fcoe fc-map *prefix* vlan *vlan_id*
no fcoe fc-map *prefix* vlan *vlan_id*
fcoe discovery-advertisement vlan *vlan_id*[*-vlan_id2*] [a-bit {enable | disable}] [fka-adv-period *adv_seconds***]** [priority *priority*] [uds-retries *retries*]
fcoe {port *chassis/slot/port***[***-port2***]** | linkagg *agg_id[-agg_id2*]} role {edge | enode-only | fcf-only | mixed | trusted | ve}
no fcoe {port *chassis/slot/port***[***-port2***]** | linkagg *agg_id[-agg_id2*]}
show fcoe
show fcoe ports
show fcoe sessions [[fips | npiv-proxy | r-npiv] [port *chassis/slot/port*] | vlan *vlan_id* | linkagg *agg_id*] | [e-tunnel [*tunnel_id*]]]
show fcoe enode [*mac_address*]
show fcoe fcf [*mac_address*]
show fcoe fc-map
show fcoe discovery-advertisement [vlan *vlan_id*[*-vlan_id2*]]
show fcoe statistics [enode | fcf] {interface | vlan [*vlan_id*[*vlan_id2*] | port *chassis/slot/port***[***-port2***]** | linkagg *agg_id[-agg_id2*]}
clear fcoe statistics [enode | fcf] [interface | vlan [*vlan_id*[*vlan_id2*] | port *chassis/slot/port***[***-port2***]** | linkagg *agg_id[-agg_id2*]]

FCoE/FC Gateway Commands

fibre-channel vsan {*vsan_id*[*-vsan_id2*]} [admin-state {enable | disable}] [name *description***]**
no fibre-channel vsan {*vsan_id*[*-vsan_id2*]}
fibre-channel port *chassis/slot/port***[***-port2***]** mode {np | f | te} [bb-sc-n *buffer_num*]
no fibre-channel port *chassis/slot/port***[***-port2***]**
fibre-channel vsan *vsan_id* members port *chassis/slot/port[-port2]*
no fibre-channel vsan *vsan_id* members port *chassis/slot/port[-port2]*
fcoe vsan-map vsan *vsan_id* vlan *vlan_id*
no fcoe vsan-map vsan *vsan_id* vlan *vlan_id*
fibre-channel npiv-proxy load-balance static {default | dynamic-reorder | enode-based}
fibre-channel npiv-proxy load-balance static {port *chassis/slot/port* | linkagg *agg_id*} fc-port *chassis/slot/port*
no fibre-channel npiv-proxy load-balance static {port *chassis/slot/port* | linkagg *agg_id*} fc-port *chassis/slot/port*
fcoe e-tunnel *tunnel_id* {fc-port1 *chassis/slot/port*} {fc-port2 *chassis/slot/port* | vlan *vlan_id*}
no fcoe e-tunnel *tunnel_id*
show fibre-channel vsan [*vsan_id*]-*vsan_id2*]
show fibre-channel vsan [*vsan_id* [*-vsan_id2]]* members [port *chassis/slot/port[-port2]]*
show fibre-channel port *[info]*
show fcoe vsan-map
show fibre-channel sessions [vsan *vsan_id* | e-tunnel *tunnel_id*] [port *chassis/slot/port***]** [summary]
show fibre-channel node [vsan *vsan_id* | port *chassis/slot/port***]**
show fcoe e-tunnel [*tunnel_id*]
show fibre-channel

show fibre-channel statistics [npiv | r-npiv] [vsan *vsan_id*[*vsan_id2*] [port *chassis/slot/port*[-*port2*] [e-tunnel port *chassis/slot/port*[-*port2*]]
show fcoe statistics npiv-proxy {enode-login | enode-discovery} {interface | vlan [*vlan_id*[*vlan_id2*] | port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]}
show fcoe statistics r-npiv {node-login | fcf-discovery} {interface | vlan [*vlan_id*[*vlan_id2*] | port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]}
show fcoe statistics e-tunnel [ve | te] [*tunnel_id*[-*tunnel_id*]]
show fibre-channel npiv-proxy load balance {static | session-count}
clear fibre-channel statistics [npiv | r-npiv] [port *chassis/slot/port*[-*port2*] [e-tunnel port *chassis/slot/port*[-*port2*]]
clear fibre-channel sessions {npiv-proxy | r-proxy | e-tunnel | all}
clear fcoe statistics npiv-proxy {interface | vlan [*vlan_id*[*vlan_id2*] | port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]}
clear fcoe statistics r-npiv {interface | vlan [*vlan_id*[*vlan_id2*] | port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]}
clear fcoe statistics e-tunnel [ve | te] {*tunnel_id*[-*tunnel_id*]}
clear fcoe sessions [fips | npiv-proxy | r-proxy | e-tunnel | all]

VXLAN Snooping Commands

vm-snooping admin-state {enable | disable}
vm-snooping policy-mode {basic | advance} [policy-resource {extended | default}] [inner-header {tagged | untagged | default}]
vm-snooping trap {enable | disable}
vm-snooping filtering-resource trap threshold {*percentage* | default}
vm-snooping sampling-rate *pps*
vm-snooping aging-timer *seconds*
vm-snooping vxlan udp-port {*udp_port_num*[-*udp_port_num2*}
no vm-snooping vxlan udp-port {*udp_port_num*[-*udp_port_num2*}
vm-snooping static-policy rule *rule_name* [list *list_name*]
no vm-snooping static-policy rule *rule_name* [list *list_name*]
vm-snooping logging-threshold number-of-flows {*flow_num* | default}
vm-snooping {port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]} [admin-state {enable | disable}]
no vm-snooping {port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]}
show vm-snooping config
show vm-snooping port
show vm-snooping database [vxlan udp-port *udp_port_num* | vtep-ip *ip_address* | vni *vxlan_id* | vm-src-mac *mac_address* | vm-ip *ip_address*] [detail] *[*port *chassis*/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*]] [detail]
clear vm-snooping database *[*port *chassis*/slot/port[-*port2*] | linkagg *agg_id[-agg_id2*]]
show vm-snooping virtual-machines
show vm-snooping filtering-resource
show vm-snooping statistics [hardware | sampling] *[*port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]]
show vm-snooping static-policy
clear vm-snooping statistics [sampling *[*port *chassis/slot/port*[-*port2*] | linkagg *agg_id[-agg_id2*]]] [hardware]

Port Mapping Commands

port-mapping session_id [user-port {slot *chassis/slot* | *chassis/slot/port*[-*port2*] | linkagg *agg_id*}] [network-port {slot *chassis/slot* | *chassis/slot/port*[-*port2*] | linkagg *agg_id*}]
no port-mapping session_id [user-port {slot *chassis/slot* | *chassis/slot/port*[-*port2*] | linkagg *agg_id*}] [network-port {slot *chassis/slot* | *chassis/slot/port*[-*port2*] | linkagg *agg_id*}]
port-mapping session_id {enable | disable}
no port-mapping session_id
port-mapping session_id [unidirectional | bidirectional]
port-mapping session_id unknown-unicast-flooding {enable | disable}
port-mapping session_id dynamic-proxy-arp {enable | disable}
show port-mapping [*session_id*] status
show port-mapping [session_id]

Learned Port Security Commands

port-security {port *chassis/slot/port*[-*port2*] | chassis} [admin-state {enable | disable | locked}]
no port-security port *chassis/slot/port*[-*port2*]
port-security learning-window *minutes* [convert-to-static {enable | disable}] [no-aging {enable | disable}] [mac-move {enable | disable}] [learn-as-static {enable | disable}] [boot-up {enable | disable}]
no port-security learning-window
port-security {port *chassis/slot/port*[-*port2*] | chassis} convert-to-static
port-security port *chassis/slot/port*[-*port2*] mac *mac_address* [vlan *vlan_id*]
no port-security port *chassis/slot/port*[-*port2*] mac [all | *mac_address*] [vlan *vlan_id*]
port-security port *chassis/slot/port*[-*port2*] maximum *number*
port-security port *chassis/slot/port*[-*port2*] learn-trap-threshold *number*
port-security port *chassis/slot/port*[-*port2*] max-filtering *number*
port-security port *chassis/slot/port*[-*port2*] mac-range [low *mac_address* | high *mac_address*]
no port-security port *chassis/slot/port*[-*port2*] mac-range [low *mac_address*]
port-security port *chassis/slot/port*[-*port2*] violation {shutdown | restrict | discard}
show port-security {port [*chassis/slot/port*[-*port2*] | slot *chassis/slot*]}
show port-security [port *chassis/slot/port*[-*port2*]] mac-range
show port-security brief
show port-security learning-window

Port Mirroring and Monitoring Commands

port-mirroring *port_mirror_sessionid* source {port *chassis/slot/port*[-*port2*]} destination {port *chassis/slot/port*[-*port2*] | *linkagg linkagg*[-*linkagg2*]*}* [rpmir-vlan *vlan_id*] [bidirectional |inport |outport] [unblocked-vlan *vlan_id*] [tag-remove] [enable | disable]
port-mirroring *port_mirror_sessionid no* source {port *chassis/slot/port*[-*port2*] [*chassis/slot/port*[-*port2*]*...}*
port-mirroring *port_mirror_sessionid no* destination {port *chassis/slot/port*[-*port2*] [*chassis/slot/port*[-*port2*]...] | *linkagg linkagg*[-*linkagg2*] *[linkagg*[-*linkagg2*]*...}*
port-mirroring *port_mirror_sessionid* {enable | disable}
no port-mirroring *port_mirror_sessionid*
port-monitoring *port_monitor_sessionid* source port *chassis/slot/port*[-*port2*] [file *filename* [size *filesize*] | no file | overwrite {on | off}] [inport | outport | bidirectional] [timeout *seconds*] [enable | disable] [capture-type {full | brief}]
port-monitoring *port_monitor_sessionid* no source port *chassis/slot/port*[-*port2*]
port-monitoring *port_monitor_sessionid* {disable | pause | resume}
no port-monitoring *port_monitor_sessionid*
show port-mirroring status [*port_mirror_sessionid*]
show port-monitoring status [*port_monitor_sessionid*]
show port-monitoring file *port_monitor_sessionid*

sFlow Commands

sflow agent ip ip_address
no sflow agent ip ip_address
sflow receiver *receiver_index* {name *string* | timeout {*seconds* | forever} | address {*ip_address* | *ipv6_address* | *domain_name*} | udp-port *port* | packet-size *size* version *num* | release}
sflow sampler *num* port *chassis/slot/port*[-*port*] {receiver *receiver_index* | rate *value* | sample-hdr-size *size*}
no sflow sampler *num* port *[chassis_id/]slot/port*[-*port*]
sflow poller *num* port *chassis/slot/port*[-*port*] {receiver *receiver_index* | interval *value*}
no sflow poller *num* port *[chassis_id/]slot/port*[-*port*]
show sflow agent
show sflow receiver [num]
show sflow sampler [*num*]
show sflow poller [*num*]

RMON Commands

rmon probes {stats | history | alarm} [*entry_number*] {enable | disable}
show rmon probes [stats | history | alarm] [*entry_number*]
show rmon events [*entry_number*]

Switch Logging Commands

swlog {enable | disable | preamble | hash-time-limit seconds | duplicate-detect | console level num }
no swlog [preamble | duplicate-detect]
swlog syslog-facility-id {*facility_id* | *num*}
swlog appid {*all* | *string*} {library {all | string} | subapp {all | num} | exclude {all | num}} {disable | enable | level {*level* | *num*} [vrf num]
swlog output {tty {enable | disable} | console | flash | socket {*ip_address* | *ipv6Address* | *domain_name*} [tls] [remote command-log] [vrf-name name]}
no swlog output {console | flash | socket [*ip_address* | *ipv6Address* | *domain_name*]}
swlog output flash-file-size *kilobytes*
swlog advanced {enable | disable}
swlog size-trap-threshold *threshold*
swlog clear [all]
show log swlog
show log swlog [timestamp mm/dd/yyyy hh:mm:ss] [slot num]
show swlog [library | appid {all | string} | dying-gasp-station]
swlog console level {*num* | alarm | alert | debug1 | debug2 | debug3 | error | info | off | warning }
show log events
show log events output *filename*

Health Monitoring Commands

health threshold {rx *percent* | txrx *percent* | memory *percent* | cpu *percent* | flash *percent*}
health interval *seconds*
show health configuration
show health [port *chassis/slot/port* | slot *chassis/slot***[**-*slot2***]]** [statistics]
show health all {memory | cpu | rx | txrx}

Ethernet OAM Commands

ethoam vlan *vlanid_list* primary-vlan *vlan_id*
no ethoam vlan *vlanid_list*
ethoam domain md_name format {none | dnsname | mac-address-uint | string} level *num*
no ethoam domain *name*
ethoam domain md_name mhf {none | explicit | default}
ethoam domain md_name id-permission {none | chassisid}
ethoam association ma_name format {vpnid | unsignedint | string | primaryvid | icc-based} domain md_name
no ethoam association *ma_name* domain *md_name*
ethoam association ma_name domain md_name primary-vlan vlan_id
no ethoam association *ma_name* domain *md_name primary-vlan vlan_id*
ethoam association *ma_name* domain *md_name* mhf {none | default | explicit | defer}

ethoam association *ma_name* domain md_name id-permission {none | chassisid | defer}
ethoam association *ma_name* domain **{***md_name* | *mac_address***}** ccm-interval {interval-invalid | interval100ms | interval1s | interval10s | interval1m | interval10m}
ethoam association *ma_name* domain **{***md_name* | *mac_add***}** endpoint-list *mep_id*[-*mep_id2***]**
no ethoam association *ma_name* domain **{***md_name* | *mac_add***}** endpoint-list *mep_id*[-*mep_id2***]**
clear ethoam statistics [domain md_name association *ma_name* endpoint mep_id]
ethoam default-domain level *num*
no ethoam default-domain
ethoam default-domain mhf {none | default | explicit}
no ethoam default-domain
ethoam default-domain id-permission {none | chassisid}
no ethoam default-domain
ethoam default-domain primary-vlan {vlan_id} [level {no-level | num}] [mhf {none | default | explicit | defer}] [id-permission {none | chassisid | defer}]
no ethoam default-domain
ethoam endpoint *mep_id* domain *md_name* association *ma_name* direction {up | down} {port *chassis/slot/port* | virtual | linkagg *agg_id*} [primary-vlan *vlan_id*]
no ethoam endpoint *mep_id* domain *md_name* association *ma_name*
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* admin-state {enable | disable}
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* rfp {enable | disable}
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* ccm {enable | disable}
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* priority *ccm_ltm_priority*
ethoam endpoint *mep_id* domain **{***md_name* | *mac_address***}** association *ma_name* lowest-priority-defect *lowest_priority_defect*
ethoam linktrace {target-macaddress *mac_address* **|** target-endpoint *t_mepid***}** source-endpoint *s_mepid* domain **{***md_name* | *mac_address***}** association *ma_name* [flag [fdb-mpdb | fdb*only]*] [hop-count *hop_count*]
ethoam loopback {target-endpoint *t_mepid* | target-macaddress *mac_address*} source-endpoint *s_mepid* domain *md_name* association *ma_name* [number num] [data string] [vlan-priority vlan_priority] [drop-eligible {true | false}]
ethoam fault-alarm-time *centiseconds* endpoint *mep_id* domain *md_name* association *ma_name*
no ethoam fault-alarm-time endpoint *mep_id* domain *md_name* association *ma_name*
ethoam fault-reset-time *centiseconds* endpoint *mep_id* domain *md_name* association *ma_name*
no ethoam fault-reset-time endpoint *mep_id* domain *ma_name* association *ma_name*
ethoam one-way-delay {target-endpoint t_mepid | target-macaddress *mac_address*} source-endpoint s_mepid domain *md_name* association *ma_name* [vlan- priority vlan_priority]
ethoam two-way-delay {target-endpoint *t_mepid* | target-macaddress *mac_address*} source-endpoint *s_mepid* domain *md_name* association *ma_name* [vlan- priority vlan_priority]
clear ethoam {one-way-delay-table | two-way-delay-table}
show ethoam
show ethoam domain *md_name*
show ethoam domain *md_name* association *ma_name*
show ethoam domain *md_name* association *ma_name* end-point *mep_id*
show ethoam default-domain configuration
show ethoam default-domain [primary-vlan *vlan_id*]
show ethoam remote-endpoint domain *md_name* association *ma_name* end-point *s_mepid* [remote-mep r_mepid]
show ethoam cfmstack {port *chassis/slot/port* | virtual | linkagg *agg_id*}
show ethoam linktrace-reply domain *md_name* association *ma_name* endpoint *s_mepid* tran-id *num*
show ethoam linktrace-tran-id domain **{***md_name* | *mac_address***}** association *ma_name* endpoint *mep_id*
show ethoam vlan vlan_id
show ethoam statistics domain **{***md_name* | *mac_address***}** [association *ma_name*] [end-point mep_id**]**
show ethoam config-error [vlan vlan_id] [{port chassis/slot/port | linkagg agg_id}]
show ethoam one-way-delay domain md_name association ma_name endpoint s_mepid [mac-address mac_address]
show ethoam two-way-delay domain md_name association ma_name endpoint s_mepid [mac-address mac_address]

LINK OAM Commands

efm-oam admin-state {enable | disable}
efm-oam port *chassis/slot/port* **[***-port2***]** admin-state {enable | disable}
efm-oam port *chassis/slot/port***[***-port2***]** mode {*active* | *passive*}
efm-oam port *chassis/slot/port***[***-port2***]** keepalive-interval *seconds*
efm-oam port *chassis/slot/port*[*-port2*] hello-interval *seconds*
efm-oam port *chassis/slot/port*[*-port2*] remote-loopback {process | ignore}
efm-oam port *chassis/slot/port* remote-loopback {start | stop}
efm-oam port *chassis/slot/port*[*-port2*] propagate-events {critical-event | dying-gasp} {enable | disable}
efm-oam port *chassis/slot/port*[*-port2*] errored-frame-period [threshold *threshold_symbols*] [window *window_frames*] [notify {enable | disable}]
efm-oam port *chassis/slot/port*[*-port2*] errored-frame [threshold *threshold_symbols*] [window *window_seconds*] [notify {enable | disable}]
efm-oam port *chassis/slot/port*[*-port2*] errored-frame-seconds-summary [threshold *threshold_seconds*] [window *window_seconds*] [notify {enable | disable}]
efm-oam multiple-pdu-count *count*
efm-oam port *chassis/slot/port* l1-ping [num-frames *number*] [delay *milliseconds*] [start]

show efm-oam configuration
show efm-oam port [*chassis/slot/port1-port2*] [enable | disable] [active | passive]
show efm-oam port *chassis/slot/port* detail
show efm-oam port *chassis/slot/port*[*-port2*] statistics
show efm-oam port statistics
show efm-oam port *chassis/slot/port* remote detail
show efm-oam port *chassis/slot/port* history [log-type { link-fault | errored-frame | errored-frame-period | errored-frame-seconds | dying-gasp | critical}]
show efm-oam port *chassis/slot/port* l1-ping detail
clear efm-oam statistics [port *chassis/slot/port*[*-port2*]]
clear efm-oam log-history [port *chassis/slot/port*[*-port2*]]

CPE Test Head Commands

test-oam *string* [descr *description*]
no test-oam *string*
test-oam *string* [direction {unidirectional | bidirectional}]
test-oam string [src-endpoint src-string] [dst-endpoint dst-string]
test-oam string port chassis/slot/port
test-oam string [vlan svlan] [[test-frame [src-mac src-address] [dst-mac dst-address]]
test-oam string role {generator | analyzer | loopback}
test-oam string [duration secs] [rate rate] [packet-size bytes]
test-oam string frame
test-oam string l2-saa [priority vlan-priority] [count num-pkts] [interval inter-pkt-delay] [continuous] [size size] [drop-eligible {true | false}]
no test-oam string l2-saa
test-oam string {[vlan vlan-id] [port chassis/slot/port] [packet-size bytes] start | stop} [fetch-remote-stats]
test-oam string remote-sys-mac string
test-oam statistics flash-logging {enable | disable}
show test-oam [tests | string]
show test-oam [string] statistics
show test-oam [string] saa statistics
clear test-oam [string] statistics
test-oam *group* string [descr *description*]
no test-oam group *string*
test-oam *group* string [tests string1.....string8]
test-oam group string [no tests string1.....string8]
test-oam *feeder-port* chassis/lot/port
no test-oam feeder-port
test-oam group string [src-endpoint src-string dst-endpoint dst-string] [src-endpoint src-string] [dst-endpoint dst-string]
test-oam group name role {generator | analyzer | loopback}
test-oam group string port chassis/slot/port
test-oam group string [direction {unidirectional | bidirectional}]
test-oam group string [duration secs] [rate rate]
test-oam group string {[port chassis/slot/port] start | stop} [fetch-remote-stats]
test-oam group string remote-sys-mac string
clear test-oam group string statistics
show test-oam group [tests | string]
show test-oam group [string] saa statistics
show test-oam group [string] statistics

PPPoE Intermediate Agent

pppoe-ia {enable | disable}
pppoe-ia {port *chassis/slot/port*[*-port2*] | linkagg agg_num} {enable | disable}
pppoe-ia {port *chassis/slot/port*[*-port2*] | linkagg agg_num} {trust | client}
pppoe-ia access-node-id {base-mac | system-name | mgnt-address | user-string string}
pppoe-ia circuit-id {default [atm] ascii [base-mac | system-name | interface | vlan | cvlan | interface-alias | user-string string | delimiter char]}
pppoe-ia remote-id {base-mac | system-name | mgnt-address | user-string string}
clear pppoe-ia statistics [port {*chassis/slot/port*[*-port2*] | linkagg agg_num]
show pppoe-ia configuration
show pppoe-ia {port {*chassis/lot/port*[*-port2*] | linkagg agg_num} [enabled | disabled | trusted | client]
show pppoe-ia {port {*chassis/slot/port*[*-port2*] | linkagg agg_num} statistics

Service Assurance Agent Commands

saa *string [*descr *description] [*interval *interval] [*jitter-threshold *jitter_thresh] [*rtt-threshold *rtt_thresh]*
no saa *string*
saa *string* type ip-ping destination-ip *ip_address source-ip ip_address type-of-service tos [num-pkts count] [inter-pkt-delay delay] [payload-size size]*
saa *string* type mac-ping destination-mac *mac_address* vlan *vlan_id* [vlan-priority *vlan_priority*] [drop-eligible {true | false}] [data *data*] [num-pkts *count]* [inter-pkt-delay *delay]* [payload-size *size]* [isid-check *isid*]
saa spb [auto-create] [auto-start] [interval interval] [vlan-priority vlan_priority] [drop-eligible {true | false}] [data data] [num-pkts count] [inter-pkt-delay delay] [payload-size size] [jitter-threshold jitter_thresh] [rtt-thresh rtt_thresh] [keep]
saa spb reset
saa spb flush
saa string type ethoam-loopback {target-endpoint *t_mepid* | target-mac address *mac_address*} source-endpoint *s_mepid* domain *md_name* association *ma_name* vlan-priority vlan_priority [drop-eligible {true | false}] [data data] [num-pkts num] [inter-pkt-delay delay]

saa string type {ethoam-two-way-delay} {target-endpoint *t_mepid* | target-mac address *mac_address*} source-endpoint s*_mepid* domain *md_name* association *ma_name* vlan-priority vlan_priority [num-pkts num] [inter-pkt-delay delay]
saa string start [at yyyy-mm-dd,hh:mm:ss.ds]
saa string stop [never | at yyyy-mm-dd,hh:mm:ss.ds]
saa xml [file-name xml_filename [interval interval] [admin-state {enable | disable}]
show saa [string | {descr description}] [owner saa_owner]
show saa [string] type {mac-ping | ip-ping | ethoam-loopback | ethoam-two-way-delay} config
show saa spb
show saa xml
show saa **[***string***]** *statistics [aggregate | history]*

CMM Commands

reload [chassis-id chassis] secondary [in [*hours*:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]
reload secondary cancel
reload [chassis-id chassis] all [in [*hours*:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]
reload all cancel
reload [chassis-id chassis] from *image_dir* {rollback-timeout *minutes* | no rollback-timeout [in **[***hours:***]** *minutes* | at *hour:minute*] [redundancy-time *minutes]}*
reload slot chassis/*slot*
reload chassis-id *chassis* [all] [in [*hours*:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]
reload chassis-id cancel
copy certified *image_dir [make-running-directory]*
issu from *image_dir [redundancy-time minutes]*
issu slot *num*
write memory [flash-synchro]
copy running certified [flash-synchro]
modify running-directory *image_dir*
copy flash-synchro
takeover [chassis]
show running-directory
show reload [[chassis-id chassis] [status | all status]
show microcode [working | certified | loaded | issu | *image_dir*]
usb {enable | disable}
usb backup admin-state {enable | disable} [key *string* | hash-key *string*]
usb auto-copy {enable | disable} copy-config {enable| disable} [key *string* | hash-key *string*]
mount [/uflash]
umount /uflash
show usb statistics
show issu status
auto-config-abort
image integrity check *image_dir* key-file *filename*
image integrity get-key *image_dir*

Chassis Management and Monitoring Commands

system contact *text_string*
system name *text_string*
system location *text_string*
system date [*mm/dd/yyyy*]
system time [*hh:mm:ss*]
system timezone [*timezone_abbrev*]
system daylight-savings-time [enable | disable]
update uboot {cmm *slot* | ni {all | *slot*} *file filename}*
update fpga-cpld {cmm {chassis/*cmm* |*all}* | ni {*chassis/ni* | daughter num} *file filename}*
reload slot *slot*
power slot *chassis/slot*
no power slot *chassis/slot*
powersupply enable [*slot*]
powersupply powersave {enable | disable}
powersupply num name string type {ALE {lo-ac | hi-ac} | phoenix-contact {48VDC | 24VDC} | third-party wattage num} [chassis-id chassis-id]
hash-control {brief | extended [udp-tcp-port] | load-balance non-ucast {enable | disable}}
hash-control extended no udp-tcp-port
bluetooth {admin-state [enable | disable] | transmit-power [low | high]}
capability profile {switch | router}
capability profile tcam mode {source-ipv6 | dest-ipv6}
capability trap-threshold {MAC | ARP} {HIGH num | LOW num}
license apply {file file_name | key license_key} [order-id order_id]
show system
show hardware info
show chassis
show cmm [*slot*]
show slot [*slot*]
show module [*slot*]
show module long [*slot*]
show module status [*slot*]
show powersupply [*slot*]
show fan [*slot*]
show fantray [*slot*]
show temperature [fabric [*index*] | slot [*index*] | fantray [*index*] | cmm [*index* | *cmm_letter*] | chassis-id *chassis*]
show hash-control [non-ucast]
show license-info
show bluetooth status

show me
show tcam utilization [*chasiss/slot*] [*chasiss/slot/tcam*]
show tcam utilization [*chasiss/slot*] [*chasiss/slot/tcam*] detail
show tcam app-groups
show capability profile
show pmd-files
show capability trap-threshold
show tech-support [layer2 | layer3 | eng [complete]]
security key-chain gen-random-key
security key *key_id* algorithm {sha256 {encrypt-key *encrypt_key* | key simple_key} start-time *mm/dd/yyyy* [*hh:mm*] [lifetime *days* [*hh:mm*]] | aes-gcm-128 {hex-key hex_key | encrypt-key {*hex* | *num*}} | aes-cmac-128 {hex-key hex_key | encrypt-key {*hex* | *num*}} keyed-name *hex-kn*}
no security key *key_id [-key_id2]*
security key-chain *key_chain_id* [name *key_chain_name*]
no security key-chain *key_chain_id1 [-key_chain_id2]*
security key-chain *key_chain_id* key *key_id [-key_id2]*
no security key-chain *key_chain_id1 [-key_chain_id2]}*
show security key *[key_id [-key_id2]]*
show security key-chain *[key_chain_id]*
alarm in *alr_in_name* [chassis-in *chassis_id_in*] action {swlog | trap | alarm-out} [admin-state {enable | disable}]
no alarm *alr_in_name*
alarm event *alr_event_name* {event {vc-status-change | temperature | system-health | power-supply | port-violation network-port *userport* [*-userport2]* | port-health | link-down network-port *userport* [*-userport2]* | authentication-failure} | trapid *id*}} [chassis-in *chassis_id_in*] [admin-state {enable | disable}]
no alarm *alr_event_name*
alarm out *alr_out_name* [chassis-out *chassis_id_out*] [admin-state {enable | disable}]
no alarm out *alr_out_name*
alarm map *alarm_name* out *alr_out_name*
no alarm map *alarm_name*
alarm duration *[[hour]* [*min]* | [default]]
alarm clear status [*alarm_name]*
show alarm input config chassis *chassis_id*
show alarm event config chassis *chassis-id*
show alarm status chassis *chassis-id*
appmgr {start | stop | restart} [ams broker | config-sync | config-dbase] [ams-apps iot-profiler]
appmgr list [*app_name*]
appmgr commit
pkgmgr {[install | verify] *package_file_name* | remove *package_name*}
pkgmgr list [*package_name*]
pkgmgr commit

Chassis MAC Server (CMS) Commands

mac-range eeprom *start_mac_address count*
show mac-range [*index*]
show mac-range [*index*] alloc

Network Time Protocol Commands

ntp server {*ip_address* | *server_name}* [key *key_id* | | minpoll *poll* | maxpoll *poll* | version *version* | prefer | burst | iburst | preempt]
no ntp server *ip_address*
ntp server synchronized
ntp server unsynchronized
ntp client admin-state {enable | disable}
ntp src-ip preferred {default | no-loopback0 | *ip_address*}
no ntp src-ip preferred
ntp broadcast-client {enable | disable}
ntp broadcast-delay *microseconds*
ntp key *key* [trusted | untrusted]
ntp key load
ntp authenticate {enable | disable}
ntp master stratum_number
ntp interface {interface_ip} {enable | disable}
ntp max-associations number
ntp broadcast {broadcast_addr} [version version] [minpoll poll_interval]
no ntp broadcast {broadcast_addr}
ntp peer {ip_address} [key key_id] [version version] [minpoll poll_interval]
no ntp peer {ip_address}
ntp vrf-name name
show ntp status
show ntp client
show ntp client server-list
show ntp server client-list
show ntp server status [*ip_address*]
show ntp keys
show ntp peers
show ntp server disabled-interfaces

Session Management Commands

session login-attempt integer
session login-timeout *seconds*
session {cli | ftp | http} banner file_name
no session {cli | ftp | http} banner

session {cli | http | ftp} timeout *minutes*
session prompt default [*string*]
session xon-xoff {enable | disable}
show prefix
user profile save
user profile reset
history *number*
!{! | *n*}
command-log {enable | disable}
kill *session_number*
exit
whoami
who
show session config
show session xon-xoff
more filename
[vrf name] telnet {port [default | service_port] | admin-state [enable | disable] | *ip_address*}
[vrf name] ssh {port [default | service_port] | admin-state [enable | disable] | *ip_address*}
ssh login-grace-time *seconds*
ssh enforce-pubkey-auth {enable | disable}
ssh strong-ciphers {enable | disable}
ssh strong-hmacs {enable | disable}
installsshkey *user path*
revokesshkey user remote-user
show command-log
show command-log status
[vrf name] show telnet
[vrf name] show ssh

File Management Commands

cd [*path*]
pwd
mkdir [*options*] [*path*] */dirname*
rmdir [*options*] *dirname*
ls [options] [path/*filename*]
rm [options] [path/*filename*]
cp [options] *source destination*
scp [*options*] *user_name@remote_ip_addr:[path/]source [path/]target*
scp [*options*] *[path/]source user_name@remote_ip_addr:[path/]target*
mv [options] *source destination*
chmod {+w | -w} [*path/]file*
freespace [/flash | /uflash]
fsck /uflash {repair | no-repair}
newfs /uflash
vi [*options*] [*path/]filename*
tty *lines columns*
show tty
tftp [*options*] host [port]
sftp [*options*] {*ip_address*}
ftp {port [default | service_port] | admin-state [enable | disable] | *ip_address}*
[vrf name] ftp admin-state [enable | disable]
[vrf name] show ftp

Web Management Commands

[vrf name] webview server {enable | disable}
[vrf name] webview access {enable | disable}
webview force-ssl {enable | disable}
webview http-port {default | port *port*}
webview https-port {default | port *port*}
webview ssl-strong-ciphers {enable | disable}
webview wlan cluster-virtual-ip precedence {lldp | configured}
webview wlan cluster-virtual-ip *virtual-ip-address-of-wlan-cluster*
show webview wlan config
[vrf name] show webview

Configuration File Manager Commands

configuration apply *filename* [at *hh:mm month dd* [*year*]] | [in *hh*[*:mm*]] [verbose]
configuration error-file-limit *number*
show configuration status
configuration cancel
configuration syntax-check *path/filename* [verbose]
configuration snapshot [*feature_list* | all} [*path/filename*]
show configuration snapshot [*feature_list*]
write terminal
configuration apply network-sync *filename* [community community-name | local-apply]

SNMP Commands

snmp station {*ip_address* | *ipv6_address* | *domain_name*} {[*port*] [*username*] [v1 | v2 | v3 | v3 tsm local-identity local_string remote-identity remote_string] [enable | disable]}
no snmp station {*ip_address* | *ipv6_address* | *domain_name*}
show snmp station [details]
snmp snmp-engineid-type {text | mac-address | ipv4-address | ipv6-address} snmp-engineid {*text_string* | *mac_address* | *ipv4_address* | *ipv6_address*}
snmp snmp-engineid-type mac-address snmp-engineid default

show snmp snmp-engineid
snmp community-map {[hash-key string | *community_string]* user *useraccount_name*} [enable | disable]
no snmp community-map *community_string*
snmp community-map mode {enable | disable}
show snmp community-map
snmp security {no-security | authentication set | authentication all | privacy set | privacy all | trap-only | tls {enable | disable}}
snmp security tsm [enable | disable]
snmp tsm-map remote-identity remote_string user user_string
show snmp tsm-map
show snmp security [tsm]
show snmp statistics
show snmp mib-family [*table_name*]
snmp-trap absorption {enable | disable}
snmp-trap to-webview {enable | disable}
snmp-trap replay-ip {*ip_address* | *ipv6_address* | *domain_name*} [*seq_id*]
snmp-trap filter-ip {*ip_address* | *ipv6_address* | *domain_name*} *trap_id_list*
no snmp-trap filter-ip {*ip_address* | *ipv6_address* | *domain_name*} *trap_id_list*
snmp authentication-trap {enable | disable}
show snmp-trap replay-ip
show snmp-trap filter-ip
show snmp authentication-trap
show snmp-trap config
event-action {trap *trigger_string* script script_string | script-time-limit num}
no event-action trap *name*
show event-action [statistics | trap *name [statistics]]*

OmniVista Cirrus Commands

cloud-agent admin-state {enable | disable | disable **force | restart**}
cloud-agent discovery-interval *minutes*
cloud-agent remove-inconsistent-certificate
show cloud-agent status
show cloud-agent vpn status

OpenFlow Commands

openflow back-off-max *seconds*
openflow idle-probe-timeout *seconds*
openflow logical-switch name [probe-time num | failure-detect-time num | tcp-buffer-size num | dpid string] [admin-state {enable | disable}] [mode {normal | api | pfc-channel}] [version {1.0 | 1.3.1}+] [learned-mac-update {enable | disable}] [vlan *vlan_id*] [table-miss-action {drop | controller}
no openflow logical-switch <name>
openflow logical-switch name controller {ip_address | *domain_name*} [:port] [priority num] admin-state {enable | disable}
no openflow logical-switch name controller {ip_address | *domain_name*} [:port]
openflow logical-switch name interfaces {port chassis/slot/port1[-port2] | linkagg agg_id[-*agg_id2*] | [type {trunk | access}] | [native-vlan vlan] | [vlan-tag vlan[-vlan2]]}
no openflow logical-switch name interfaces {port chassis/slot/port1[-port2] | linkagg agg_id[-*agg_id2*]}
show openflow
show openflow logical-switch [name | controllers | interfaces [vlans | port | linkagg] | details]

DNS Commands

ip domain-lookup
no ip domain-lookup
ip name-server *server_address1* [*server_address2* [*server_address3*]]
ipv6 name-server *server_ipv6_address1* [*server_ipv6_address2* [*server_ipv6_address3*]]
ip domain-name *name*
no ip domain-name
show dns

Index

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W